PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA EL DESPLIEGUE DE LA PLATAFORMA IIoT DE AIGÜES DE BARCELONA

ÍNDICE

1 INTRODUCCIÓN....5
1.1 Nuevos requerimientos de información operacional....5
1.2 Proyecto RESSONA de Aigües de Barcelona....5
2 CONTEXTO....8
2.1 Plataforma IIoT....8
2.2 Aplicaciones Edge Computing en plataformas IIoT....9
2.3 Seguridad por diseño....9
2.3.1 Zona de operación....10
2.3.2 Zona desmilitarizada DMZ....11
2.3.3 Zona corporativa....11
3 OBJETIVOS....12
4 ALCANCE....14
5 ARQUITECTURA DE LA PLATAFORMA IIoT....18
5.1 Arquitectura por tipo de site....18
5.2 Arquitectura por subsistemas....19
5.2.1 Sistema de orquestación (morado)....20
5.2.2 Sistema de ingesta (verde)....21
5.2.3 Sistema de armonización y estructuración de datos (naranja)....22
6 REQUERIMIENTOS TÉCNICOS DE EJECUCIÓN....24
6.1 Lote 1: Requerimientos técnicos ámbito SCI-OT....24
6.1.1 Hardware del sistema: Industrial PC....24
6.1.2 Sistema de orquestación (RFO)....28
6.1.3 Sistema de ingesta (RSI)....31
6.1.4 Plataforma de IIoT (RO)....34
6.1.5 Licencias plataforma IIoT....39
6.1.6 Sistema de data streaming....40
6.1.7 Requisitos de implementación....43
6.2 Lote 2: Requerimientos técnicos ámbito TI y ciberseguridad....46
6.2.1 Implementación de servidores ESXi CPD....46
6.2.2 Ampliación servidores EDAR....47
6.2.3 Requisitos Hardware CPD....47
6.2.4 Mantenimiento hardware y licencias para el CPD....48
6.2.6 Servicios profesionales CPD....48
6.2.7 Requisitos Hardware Sant Feliú de Llobregat y Gava-Viladecans....49
6.2.9 Mantenimiento hardware y licencias para Sant Feliú de Llobregat y Gava-Viladecans....50
6.2.10 Ampliación Sant Feliu y Gavá para Hiperconvergencia....50
6.2.11 Requisitos Hardware Montcada i Reixac....51

6.2.13 Mantenimiento hardware y licencias Montcada i Reixac..... 52
6.2.14 Ampliación Montcada i Reixac para Hiperconvergencia..... 52
6.2.15 Servicios Profesionales EDARS (SF, Gavá, Montcada)..... 52
6.2.16 Requerimientos técnicos ciberseguridad..... 54
6.2.17 Ciberseguridad equipos OT..... 54
6.2.17.1 Fortificación servidores y clientes de operación..... 55
6.2.17.2 Detección de malware avanzado y respuesta a incidentes..... 56
6.2.18 Ciberseguridad de equipos IT..... 57
6.2.18.1 Fortificación servidores y clientes de operación..... 57
6.3 Lote 3: Gestor del Proyecto (PMO)..... 58
6.3.1 Obligaciones del PMO..... 58
7 CONDICIONES OPERATIVAS DE EJECUCIÓN..... 61
7.1 Lote 1: Condiciones operativas en el ámbito de SCI-OT..... 61
7.1.1 Cobertura del servicio..... 61
7.1.2 Metodología de trabajo..... 61
7.1.3 Equipo de trabajo..... 61
7.1.4 Entregables..... 63
7.1.5 Formación..... 63
7.1.6 Control de calidad..... 64
7.2 Lote 2: Condiciones operativas en el ámbito de TI y ciberseguridad de la plataforma IIoT 64
7.2.1 Cobertura del servicio..... 64
7.2.2 Metodología de trabajo..... 64
7.2.3 Equipo de trabajo..... 65
7.2.4 Entregables..... 66
7.2.5 Control de calidad..... 66
7.3 Lote 3: Condiciones operativas PMO..... 66
7.3.1 Cobertura del servicio..... 66
7.3.2 Metodología de trabajo..... 66
7.3.3 Equipo de trabajo..... 67
7.3.4. Entregables..... 68
7.3.5 Control de calidad..... 69
8 PLAZO DE ENTREGA..... 70
8.1 Planificación y plazo de entrega lote 1 (OT)..... 70
8.2 Planificación y plazo de entrega lote 2 (TI y ciberseguridad)..... 70
8.3 Planificación y plazo de entrega lote 3 (PMO)..... 70
9 GARANTÍA..... 71
9.1 Garantía suministros y servicios lote 1 (OT)..... 71
9.2 Garantía suministros y servicios lote 2 (TI y ciberseguridad)..... 71
9.3 Garantía servicios lote 3 (PMO)..... 71
10 GESTIÓN DEL SERVICIO..... 72
10.1 Dirección del Servicio..... 72

10.2 Responsable del Contrato..... 73
10.3 Jefe/a de Proyecto..... 73
10.4 Comités de Seguimiento..... 74
10.4.1 Comité de Seguimiento del Contrato..... 74
10.4.2 Comité de Seguimiento del Proyecto..... 74
11 SUBCONTRATACIÓN..... 76
12 SEGURIDAD Y SALUD LABORAL..... 77
13 OTROS REQUERIMIENTOS Y SEGUIMIENTO PERTE..... 78
13.1 Entregables..... 78
13.2 Acciones formativas..... 78
13.3 Ubicación..... 79
13.4 Recursos Materiales..... 79
13.5 Registro, control y resolución de incidencias..... 80
13.6 Acceso..... 81
13.7 Idioma..... 81
14. SEGURIDAD DE LA INFORMACIÓN..... 82
Anexo 1: Normas de seguridad IT de Aigües de Barcelona (.pdf)..... 83
Anexo 2: Seguridad en sistemas OT (.pdf)..... 84
Anexo 3: Ciberseguridad en dispositivos IIoT (.pdf)..... 85
Anexo 4: Datos a enviar a sistema IIoT (Hojas de cálculo de Google)..... 86
Anexo 5: Planificación (.pdf)..... 87
Anexo 6: Presupuesto (.pdf)..... 88
Anexo 7: Modelo de acta (.pdf)..... 89

1 INTRODUCCIÓN

1.1 Nuevos requerimientos de información operacional

El avance tecnológico de los últimos años en los sistemas de control industrial de Aigües de Barcelona, así como la necesidad de disponer cada vez más información que aporte valor a los procesos de explotación y permita la toma de decisiones basada en datos, hacen necesario disponer de una plataforma que integre toda esta información, permita la gestión y monitorización de los activos y sirva como base a los procesos analíticos de mejora y de ayuda a la decisión ubicados en capas superiores.

Tradicionalmente todo el flujo de información que recoge el estado de sensores y actuadores se ha integrado siguiendo la verticalidad:

Sensor → Controlador → Scada → Sistemas de Información

Este flujo provoca una cierta ineficiencia para aquellos casos en los que la información no requiere ser tele-controlada o supervisada desde un SCADA. Este es el caso de las iniciativas de sensorización propuestas en las actuaciones del PERTE en el ámbito del saneamiento de Aigües de Barcelona, donde se requerirá integrar toda la información para su posterior tratamiento y envío a los diferentes sistemas de información o de ayuda a la decisión, sin control ni supervisión por parte del SCADA ni de los controladores.

1.2 Proyecto RESSONA de Aigües de Barcelona

En el contexto de la primera convocatoria de subvenciones para proyectos de mejora de la eficiencia del ciclo urbano del agua, que se enmarca en el desarrollo de las actuaciones del PERTE de digitalización del ciclo del agua y de la Componente 5 del Plan de Recuperación, Transición y Resiliencia centrándose en el ciclo urbano del agua; Aigües de Barcelona, Empresa Metropolitana de Gestión del Ciclo Integral del Agua, S.A. (en adelante Aigües de Barcelona o AB) ha presentado el proyecto RESSONA a esta primera convocatoria con diversas actuaciones orientadas a la aceleración de la transformación digital, como palanca para mejorar la sostenibilidad y la resiliencia de la gestión del ciclo del agua en los municipios del área metropolitana de Barcelona, incluyendo tanto el abastecimiento como el saneamiento.

En particular, en el ámbito del saneamiento, se han propuesto actuaciones enfocadas a la eficiencia y sostenibilidad en el saneamiento y al bienestar de las masas de agua del Dominio Público Hidráulico (DPH):

a) **Eficiencia y sostenibilidad en el saneamiento**

i) **Actuación 5: Gemelo digital de la red de saneamiento:**

- Tiene como objeto aumentar el conocimiento de las infraestructuras que conforman la red y su funcionamiento en diversos escenarios, que

permitan una mejora de la toma de decisiones y se incremente la resiliencia de las infraestructuras mediante la mitigación de los riesgos.

- Se creará un gemelo digital de la red de saneamiento en alta del sistema Baix Llobregat basado en un modelo hidráulico y de calidad, y en los datos generados en las actuaciones de sensorización (A6, A8), pluviométricos/radar, de caudal circulante por la red y efluente de EDAR, de nivel en puntos de la red, de calidad, estado de bombeos, históricos, etc.

ii) Actuación 6: Despliegue de sensórica en la red de saneamiento y depuración:

- Disponer de información sobre la pluviometría, sobre los caudales y la calidad de las aguas residuales (pH, conductividad y T, O2, SST, redox, NH4+), así como de los consumos de energía, en diferentes etapas de los sistemas de saneamiento, que permitan una mejora de la gestión y mitigación de los riesgos, una mayor resiliencia a eventos extraordinarios, aumenten la eficiencia energética y la eficiencia operativa.

iii) Actuación 7: Gestión avanzada de la red de saneamiento, depuración y regeneración:

- Implementación de plataformas digitales para la monitorización y el control de la eficiencia de los procesos. Implementación sistema de información integrador de información técnica asociada al saneamiento (SITEC), plataforma control avanzado aireación (EDAR Gavá), plataforma gestión eficiente energía EDAR/ERA/EBAR, cuadros de mando (calidad y cantidad) y el control avanzado de eventos de los sistemas de saneamiento.

b) Bienestar de las masas de agua del DPH

i) Actuación 8: Despliegue de sensórica en puntos de vertido:

- Caracterización de la cantidad y la calidad (pH, conductividad, T, SST, DQO, nitratos) según requerimientos DPH de los vertidos asociados a las estaciones depuradoras y los alivios de los sistemas de saneamiento en alta en tiempo de lluvia, a fin de mejorar la gestión y la mitigación de los riesgos y la resiliencia frente a eventos extraordinarios.

En el marco de las actuaciones anteriores, se desarrollará una iniciativa para la implantación de la infraestructura de hardware y software para la monitorización, control y gestión de activos de

las Tecnologías de Operación (OT) y canalizar el flujo de datos hacia las plataformas avanzadas de operación.

En esta iniciativa, se plantea la construcción y despliegue de una plataforma *Industrial Internet of Things* (IIoT) que tiene como objeto centralizar el flujo de datos generado por la sensorización desplegada en las actuaciones 6 y 8 (caudal, calidad, energía) presentando dicha información en una única interfaz, habilitando procesos de monitorización, análisis y gestión de activos en el ámbito de las Tecnologías de Operación (OT) y a su vez, canalizar dicha información hacia plataformas superiores como puedan ser sistemas de información operativos o software de ayuda a la decisión existentes en Aigües de Barcelona como SITec (Actuación A7) u otros implementados en otras actuaciones como el gemelo digital red de saneamiento (Actuación A5), conectando así las fuentes origen de datos con los sistemas destino.

2 CONTEXTO

2.1 Plataforma IIoT

Una plataforma IIoT está formada por una infraestructura de hardware y/o software que tiene como objeto presentar, de forma centralizada, una única interfaz para la monitorización, análisis y gestión de activos en el ámbito de las Tecnologías de Operación (OT), así como canalizar el flujo de información de diferentes fuentes de datos (sensor, actuador, controlador, SCADA, …) hacia plataformas superiores como puedan ser sistemas de información técnicos o software de ayuda a la decisión.

Actualmente, dos de las principales empresas de automatización a nivel mundial como son Schneider, PTA (Rockwell) o Siemens, con sus plataformas “Siemens Industrial Edge” y “Thingworx” respectivamente, están compitiendo por posicionarse en el mercado como líderes en plataformas IIoT. Existen otro conjunto no menor de empresas de automatización que disponen de plataformas de IIoT que, de forma vertical, dan una solución específica a un subconjunto de requerimientos del mercado; no obstante, el objetivo de la plataforma IIoT objeto del presente pliego es disponer, de forma modular y flexible, de una plataforma compuesta por una infraestructura de hardware/software que sea capaz de dar solución a cualquier requerimiento de IIoT que se presente dentro del ámbito de las tecnologías de la operación, en concreto deberá:

- Proveer de toda información de OT que sea necesaria para aplicaciones de gestión y ayuda a la explotación de una forma única, contextualizada, ordenada y garantizando la seguridad.

- Reducir costes de desarrollo a medida por la conectividad de los aplicativos.

- Reducir costes de mantenimiento en el despliegue del software.

- Reducir tiempos en incidencias por falta de datos en capas superiores o fallas en el flujo de datos en capas inferiores.

- Permitir desplegar de forma segura algoritmos avanzados de control en tiempo real que necesitan cerrar el lazo de control.

- Permitir disponer de información de los activos presentada en diferentes vistas o cuadros de mando.

- Agilizar la integración de nuevas funcionalidades (software de ayuda a la decisión, algoritmos avanzados, integración de nuevos dispositivos, etc.)

2.2 Aplicaciones Edge Computing en plataformas IIoT

El EDGE Computing puede definirse como la tecnología que permite la implementación de manejo de datos, operaciones, monitorización y análisis en la fuente del equipo, sin depender de un sistema de red central. Este proceso informático distribuido optimiza el sistema ciberfísico, los dispositivos IIoT y las aplicaciones, acercando las capacidades informáticas al borde de la red (en el sitio de creación de los datos).

El principal beneficio de la informática perimetral industrial EDGE es la capacidad de llevar la informática de baja latencia a las instalaciones de producción. La tecnología EDGE llega también a los dispositivos IIoT, lo que permite:

- Eliminar los retrasos en la comunicación y el procesamiento para impulsar la automatización en tiempo real.

- Automatizar los procedimientos de mantenimiento. Un objetivo fundamental de la Industria 4.0 es la necesidad de introducir el mantenimiento predictivo en las plantas de producción. Todos los fabricantes de equipos están introduciendo dispositivos habilitados para IIoT que se pueden monitorear y reparar de forma remota sin intervención humana. IIoT sirve como un bloque de construcción fundamental para habilitar este nuevo paradigma operativo; brindando un acceso, a los fabricantes, a los equipos implementados en los sitios de sus clientes. Edge Computing puede garantizar que el procedimiento de mantenimiento de los dispositivos IIoT, esté completamente automatizado, dado que el dispositivo sabe cuándo pedir reemplazo, recarga, reparación, etc. Edge puede habilitar varias acciones correctivas en el equipo IIoT, como ejecutar verificaciones de diagnóstico, informar elevando las órdenes de trabajo de mantenimiento e iniciando las compras de componentes de reemplazo, lo que permitirá que los fabricantes de equipos y los clientes se concentren en el análisis para mejorar el rendimiento general de los equipos y procesos.

- Mejora de la seguridad de TI. El crecimiento de los dispositivos IIoT ha creado lagunas de seguridad por la aparición de varios puntos de la red IIoT, que son vulnerables debido a la falta de funciones de seguridad incorporadas. La aplicación de EDGE para IIoT es una forma eficaz, de abordar estos desafíos de seguridad. EDGE proporciona el aislamiento necesario para hacer que la red sea más tolerante a fallos, autorreparable y resistente. Además los dispositivos IIoT con EDGE capturarán, analizarán y descartarán datos temporales, mientras envían solo datos clave/permanentes a un servidor centralizado, lo que reduce los costos generales de ancho de banda, mejora la seguridad y hace que las redes sean más tolerantes a fallos.

2.3 Seguridad por diseño

Otro de los criterios de diseño esenciales, que se han marcado para la creación de la nueva arquitectura de digitalización, es la seguridad por diseño. Para ello se ha realizado una clasificación de los diferentes activos, para realizar la integración de la solución siguiendo los criterios de diseño marcados en la normativa IEC62443. Esta normativa marca el modelo de Purdue como modelo a seguir en la clasificación de activos y se utilizó como modelo conceptual para la segmentación de la red en Sistemas de Control Industrial. Muestra las interconexiones e interdependencias de todos los componentes principales de un Sistema de

control industrial (ICS) típico, dividiendo la arquitectura del ICS en dos zonas: tecnología de la información (IT) y tecnología operativa (OT), y subdividiendo estas zonas en seis niveles que comienzan en el nivel 0.

En la base del modelo de Purdue está el OT, los sistemas utilizados en infraestructuras críticas y fabricación para monitorear y controlar equipos físicos y procesos operativos. En el modelo de Purdue OT está separado de la zona de IT.. En el medio, encontramos una DMZ para separar y controlar el acceso entre las zonas de IT y OT.

Teniendo en cuenta los requisitos definidos por la especificación IEC62443-3-2 y las recomendaciones para evitar la comunicación no deseada, se comprende la necesidad de crear tres grandes zonas: zona de operación, zona desmilitarizada y zona corporativa.

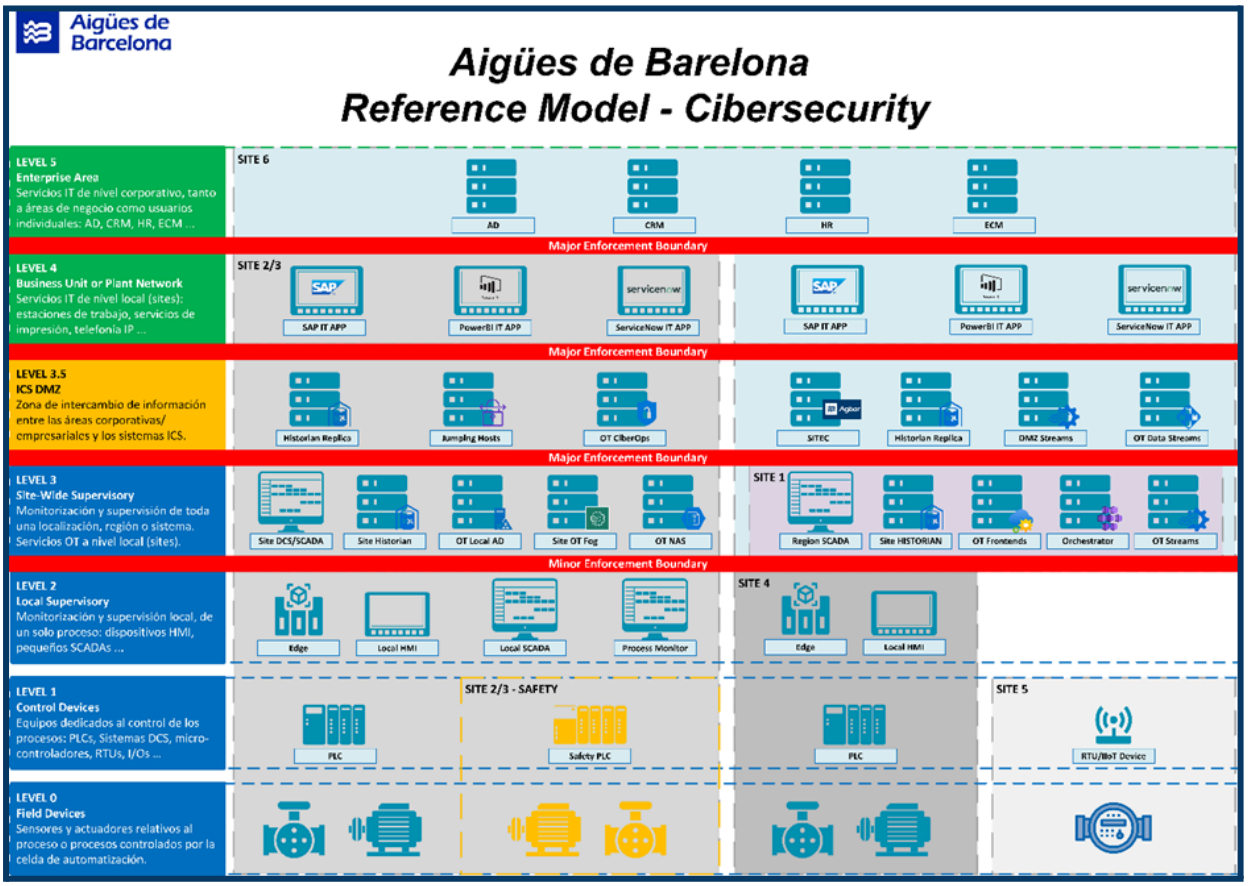


Figura 1. Modelo de referencia PURDUE

2.3.1 Zona de operación

Esta zona se encuentra dividida en 4 niveles funcionales de acuerdo con el esquema de referencia de Purdue, definido en la normativa IEC-62264-1, que se identifican así:

- Level 0: este nivel incluye a los sensores que obtienen las señales del proceso (válvulas, compresores, termómetros…). Estos dispositivos no tienen que están gobernados por elementos de control situados en el nivel 1. Dependiendo de la funcionalidad operativa

dentro del sistema, es decir, dependiendo del tipo de site se contemplarán diferentes requisitos de seguridad, por ejemplo, en las site 2/3 se incluirán requisitos Safety.

- Level 1: incluye a los dispositivos de control que gobiernan el proceso productivo de las instalaciones y realizan las funciones específicas de la ubicación o site. Únicamente los dispositivos que se encuentran en este nivel tienen acceso a los sensores de instrumentación que se encuentran en el nivel inferior y envían los datos necesarios a los niveles superiores. Los dispositivos y los requisitos de seguridad dependen del tipo de site, en las site 2/3 los dispositivos son dispositivos en algunos casos incorporan mecanismos de seguridad o safety y en las site 5 son dispositivos RTU, que envían los datos al nivel 3 de las sites 1/6 y a la nube.
- Level 2: incluye todos los dispositivos encargados de monitorizar y de recibir los datos de campo de forma local. Este nivel sólo está disponible en los sites 2, 3 y 4. Las sites 2/3 estarán compuestas por un sistema Edge, los HMI locales, el SCADA local y el monitor de procesos. En estas estaciones el nivel 2 manda los datos al nivel 3 de la estación. Las sites 4 estarán compuestas por el sistema Edge y los HMI locales, estas estaciones envían la información directamente al nivel 3 de las sites 1/6 o en el caso de que estén integradas en sites 2/3 los datos se envían también al nivel 3 de dichas estaciones.
- Level 3: incluye todos los dispositivos encargados de la monitorización y supervisión de todo un sistema. Este nivel recibe los datos del sistema. En las sites 2/3 recibe los datos de toda la estación, incluyendo las sites 4 asociadas. Este nivel estará compuesto por un sistema de supervisión SCADA y las bases de datos de las aplicaciones locales de la estación. Recibe los datos del nivel 2 de la estación local y las ubicaciones tipo 4 asociadas y los envía al nivel 3 de las sites 1/6. En las sites 1/6 este nivel estará compuesto por un sistema SCADA regional, bases de datos, los sistemas de telecontrol, un sistema de orquestación y el sistema Edge. Estos sistemas reciben los datos de los niveles inferiores de todas las estaciones remotas.

2.3.2 Zona desmilitarizada DMZ

La siguiente zona de servidores, se trata de una zona desmilitarizada, DMZ (Demilitarized Zone), la cual se encuentra en las sites 1/6 y las 2/3. Esta zona es una barrera entre las redes IT y OT evitando una comunicación directa entre redes. En este nivel se recoge toda la información de los niveles inferiores y es donde se produce el intercambio de información entre las redes IT y OT.

2.3.3 Zona corporativa

La zona corporativa (Business Zone) comprende el nivel corporativo y está clasificada como la capa de nivel 4/5. Existe una segregación lógica entre los niveles de las capas pertenecientes a IT y los niveles pertenecientes a las capas de OT. Esto asegura que los sistemas críticos de la empresa estén protegidos de los posibles ataques externos y que los datos y procesos pertenecientes a la red OT se gestionan de forma segura y eficiente. Entre los niveles de la infraestructura OT e IT se sitúa una DMZ en la que se integran todos los sistemas que tienen que ofrecer datos de OT a sistemas de los niveles superiores. Estos niveles se encuentran únicamente en los sites 1/6 y 2/3.

3 OBJETIVOS

La ingesta de datos es un proceso crítico en cualquier proyecto que requiera la recopilación de información en tiempo real, su clasificación, tratamiento y transformación, y análisis, especialmente en el caso de la tipología de infraestructura que tiene el sector de aguas. En estos proyectos, la facilidad de subida de datos es un factor clave para garantizar que la información esté disponible sin una elevada inversión inicial que garantice el acceso al dato para la gestión y análisis de la información, lo que a su vez puede ayudar a optimizar los procesos y mejorar el rendimiento general de la planta.

Los principales objetivos del proyecto están relacionados con la disponibilidad de los datos de las plantas, así como simplificar su subida:

- **Conectividad de dispositivos:** proporcionar la capacidad de conectar y comunicarse con una amplia variedad de dispositivos industriales, sensores y máquinas, incluidos sistemas heredados.
- **Automatizar la ingesta y almacenamiento de datos:** para simplificar la recolección y subida de datos, minimizar el tiempo y los recursos necesarios para hacerlo. Al automatizar el proceso, se pueden reducir errores humanos y mejorar la calidad de los datos recopilados.
- **Simplificar la integración de sistemas:** para que los datos se puedan recopilar y subir de manera más eficiente y efectiva, evitando problemas de compatibilidad y asegurar que todos los datos estén disponibles en un solo lugar para su análisis y procesamiento.
- **Integración e interoperabilidad:** admitir la integración de diferentes sistemas, protocolos y formatos de datos, permitiendo una comunicación sin problemas y la interoperabilidad entre diversos dispositivos industriales, aplicaciones y bases de datos.
- **Accesibilidad de los datos:** para que se puedan subir fácilmente desde diferentes dispositivos y plataformas. Por ello se realizará un diseño de infraestructura que pueda ofrecer los datos a aplicaciones de todos los niveles. También se integrarán módulos que permitan el envío de datos a aplicaciones en ejecución en el cloud.
- **Calidad de los datos:** implementar medidas para verificar la integridad y precisión de los datos. Esto incluye la validación de los datos en el origen antes de la subida y la realización de pruebas de calidad después de la subida para asegurar que los datos sean coherentes y útiles.
- **Establecer un estándar de subida de datos:** asegurar que los datos recopilados sean coherentes, precisos y compatibles con otros sistemas, lo que permite su análisis y comparación de manera efectiva.
- **Tratamiento de datos:** el sistema debe ofrecer la capacidad de realizar un procesamiento de datos básico en el Edge para permitir el despliegue de aplicaciones “Standalone”.
- **Análisis y visualización de datos:** ofrecer herramientas y capacidades para analizar y visualizar los datos recopilados, proporcionando información y conocimientos accionables para la toma de decisiones.
- **Monitoreo y control remoto:** permite el monitoreo y control remoto de dispositivos y procesos industriales, brindando visibilidad en tiempo real y la capacidad de realizar ajustes o tomar acciones preventivas.
- **Sistema modular:** el sistema debe estar diseñado con elementos modulares de tal forma que cualquiera de ellos pueda ser sustituido sin afectar al funcionamiento del resto de sistemas que forman la plataforma.

- **Escalabilidad y flexibilidad:** la plataforma debe estar diseñada para adaptarse a las crecientes necesidades y requisitos de los entornos industriales, acomodando un número creciente de dispositivos y volúmenes de datos en expansión.

4 ALCANCE

Se pretende construir una plataforma IIoT compuesta por una infraestructura hardware y software que recoja toda la información (ingesta de datos) de sensórica (caudal, calidad, energía y otras), permita la monitorización, control y gestión centralizada de tales elementos y a la vez provea de la información necesaria a las iniciativas de explotación de datos, algoritmos de control avanzados, software de ayuda a la decisión, software de modelización dinámica de la red de saneamiento, etc. La siguiente tabla muestra el flujo de datos entre las fuentes origen y el destino de tales sistemas.

ACTUACIÓN	ORIGEN DATOS		DESTINO DATOS
A6. SENSORIZACIÓN DE LOS SISTEMAS DE SANEAMIENTO EN ALTA DEL ÁREA METROPOLITANA DE BARCELONA EN LA CUENCA DEL LLOBREGAT	Medición de caudales de la red saneamiento del sistema Baix Llobregat		Sistemas de Gestión Avanzada de la red de saneamiento, depuración y regeneración: • Gemelo digital red de saneamiento • Sistema de Información Técnico Ecofactorias (SITec) • Plataforma gestión aireación: CREApro® • Plataforma Monitorización Avanzada Consumos Eléctricos • Dinapsis Control Data Center • Otros
	Medición de caudales EBARs del sistema Baix Llobregat		
	Estaciones de calidad control de vertidos		
	Detección entrada agua de mar sistema Baix Llobregat		
	Detección entrada aguas blancas		
	Pluviómetros		
	Medición de caudales entrada EDARs del Baix Llobregat, Gavá-Viladecans, Sant Feliú		
	Estaciones de calidad del agua residual de entrada EDARs del Baix Llobregat, Gavá-Viladecans, Sant Feliú EDARs del Baix Llobregat, Gavá-Viladecans, Sant Feliú, ERA del Baix Llobregat y EBAR Avantport Sud		
	Analizadores de consumo eléctrico de principales motores de las EDARs del		
A8. SENSORIZACIÓN DE LOS VERTIDOS Y ALIVIOS DE LOS SISTEMAS DE SANEAMIENTO EN ALTA DEL ÁREA METROPOLITANA DE BARCELONA	Medición caudales alivios red de saneamiento		
	Medición caudales alivios EBARs		
	Estaciones de calidad caracterización alivios		
	Medición caudales vertido EDARs DPH		
	Estaciones de calidad caracterización vertidos DPH		
	Medición caudales alivios EDARs		

Tabla 1. Relación del origen y el destino de datos sobre la plataforma IIoT

Independientemente de la plataforma concreta de IIoT el alcance de las diferentes tareas a desarrollar en el despliegue de dicha plataforma incluyen una serie de actuaciones como:

Ingeniería de detalle

- Análisis de las fuentes de datos origen y destino.
- Análisis de los diferentes casos de uso de las iniciativas (como mínimo se analizará el gemelo digital de la red de saneamiento, SITec saneamiento, CREApro®, Dinapsis Control Data Center y la Monitorización avanzada de consumos eléctricos).
- Análisis de los protocolos e infraestructuras de comunicaciones necesarias para recoger los datos desde los diferentes orígenes (sensores, actuadores, dataloggers, controladores, bases de datos, Scada, etc.).
- Análisis de la arquitectura de los diferentes tipos de *sites* (red de saneamiento,EBAR's, EDAR's, etc.) y la conexión entre ellos y con el centro de proceso de datos (CPD).
- Análisis de la capa de ciberseguridad sobre las diferentes opciones en cuanto a plataforma IIoT.
- Análisis de la necesidad de tratamiento de los datos: pre-procesamiento, integración, o filtrado.
- Análisis de los requerimientos de diseño: memoria, almacenamiento o velocidad de cómputo, así como la distribución del hardware y/o software entre los diferentes *sites*.
- Propuesta de las diferentes opciones de plataforma IIoT con tabla comparativa técnico-económica resultado del proceso de captura y análisis de la información.
- Análisis de la configuración de los activos.
- Análisis de la definición de las pantallas de visualización y monitorización de la información.
- Análisis de los cuadros de mando de la información recogida en la sensorización del PERTE y datos de otras fuentes de información operativas (SCADA y otras); y de los cuadros de mando para monitorizar todo el flujo de datos, hardware, software, servicios, APIS, etc.

Suministro e instalación del hardware y/o software

- Suministro de todas las licencias necesarias para el despliegue, como puedan ser sistemas operativos, bases de datos, driver, la plataforma IIoT del proveedor finalmente seleccionado, etc.
- Suministro de todo el hardware detallado e instalación en los diferentes sites.
- Instalación y configuración de software base, como puedan ser sistemas operativos, base de datos, etc.
- Aplicación de criterios de seguridad al hardware y software instalado en base a los estándares de Aigües de Barcelona.
- Suministro de los diferentes drivers y desarrollo de aquellos que son necesarios para establecer comunicación entre las diferentes plataformas.

Programación

- Tareas de filtrado, agregados y contextualización de la información.
- Pequeñas actuaciones de adaptación de la programación en controladores, Scada y otros para adecuar los flujos e ingesta de datos .
- Coordinar y establecer los criterios para la programación en los controladores, Scada y otros para configurar los flujos e ingesta de datos .
- Programación de las pantallas de visualización y monitorización de la información. Cómo mínimo se implementarán pantallas de la sensórica implementada en las actuaciones A6 y A8, ver apartado 1.2 del presente documento, por sistema de

saneamiento de la red, EBAR's y EDAR's, para los sensores de caudal, calidad, niveles, monitorización de energía, pluviómetros, etc.
- Realización de cuadros de mando por sistema de saneamiento para cada una de las iniciativas de las actuaciones A6 y A8 mencionadas.
- Realización de los cuadros de mando para monitorizar todo el flujo de datos, hardware, software, servicios, APIS, etc. La idea es tener una visión de forma rápida del flujo de los datos y de la garantía del dato , que en caso de anomalía será notificada vía alarma a los usuarios mantenedores.

Configuración de la plataforma

- Configuración de los diferentes enlaces al origen de los datos
- Integración de todos los activos, implementados en las actuacions A6 y A8 y algunos otros del SCADA, a la plataforma: sensores, actuadores, controladores.
- Securización de la plataforma.

Puesta en marcha de la plataforma

- Pruebas de rendimiento
- Pruebas de verificación o SAT (*site accept test*)

Documentación

- Diagramas (*layouts*).
- Manuales de usuario.
- Manuales de explotación y mantenimiento.
- Memoria proyecto.

Formación

- Realización de formación, tanto a los explotadores operativos de la plataforma, como a los mantenedores.

Las principales ubicaciones de ejecución del proyecto serán las siguientes:

- EDAR Baix Llobregat
- EDAR Besós
- EDAR Gavá-Viladecans
- EDAR Montcada i Reixac
- EDAR Sant Feliú de Llobregat
- CPD de Aigües de Barcelona

Las actuaciones que forman parte del ámbito del presente procedimiento de contratación han sido agrupadas, en función de sus características y/o peculiaridades técnicas, en 4 lotes:

- **LOTE 1** – ÁMBITO SISTEMAS DE CONTROL INDUSTRIAL (SCI) O TECNOLOGÍAS DE OPERACIÓN (OT) DE LA PLATAFORMA IIoT.

- **LOTE 2** - ÁMBITO DE TECNOLOGÍAS DE LA INFORMACIÓN (TI) Y CIBERSEGURIDAD DE LA PLATAFORMA IIoT.

- **LOTE 3** - GESTOR DEL PROYECTO (PMO) PARA LA IMPLANTACIÓN DE LA PLATAFORMA IIoT.

5 ARQUITECTURA DE LA PLATAFORMA IIoT

5.1 Arquitectura por tipo de site

La figura 2 muestra un esquema simplificado de la distribución geográfica de la implementación de la plataforma IIoT atendiendo a los diferentes tipos de *site* definidos en Aigües de Barcelona.

El tipo de ***site* 2** corresponde a una planta de tratamiento donde se dispone de un Scada local con sus respectivas bases de datos, donde existen controladores distribuidos por toda la planta que gobiernan y controlan los diferentes procesos y además se dispone de paneles HMI capaces de controlar las instalaciones de forma local a modo de botonera a pie de máquina. Los ejemplos que se tienen de *site* 2 en saneamiento son las 5 estaciones depuradoras de agua residual (EDAR) distribuidas por el área metropolitana de Barcelona.

El tipo de ***site* 3** corresponde a las estaciones de bombeo de agua residual (EBAR) donde no se dispone de Scada local y en muchos casos ni tan solo de HMI; en este tipo de *site* el proceso es simple y está gobernado por un controlador local que funciona de forma independiente al *site* 2 al cual pertenece.

Distribuidos geográficamente se sitúan los tipos de ***site* 5**, que corresponde a un tipo de sensor o analizador alimentado normalmente de forma autónoma (baterías) que guarda sus datos históricos en un registrador o *data logger* y tiene capacidad de transmitir esos datos referentes a la medida hacia un Scada, controlador o la plataforma IIoT.

Por último, el tipo de ***site* 6,** cuyo propósito es centralizar la información de los diferentes *sites* para ser tratada en el ámbito de las tecnologías de la información (IT), como procesos software de extracción, transformación y carga (ETL) o sistemas de información técnica en entorno de Aigües de Barcelona (*On-Premises*), así como la centralización de información en entornos externos a la compañía (Cloud de terceros).

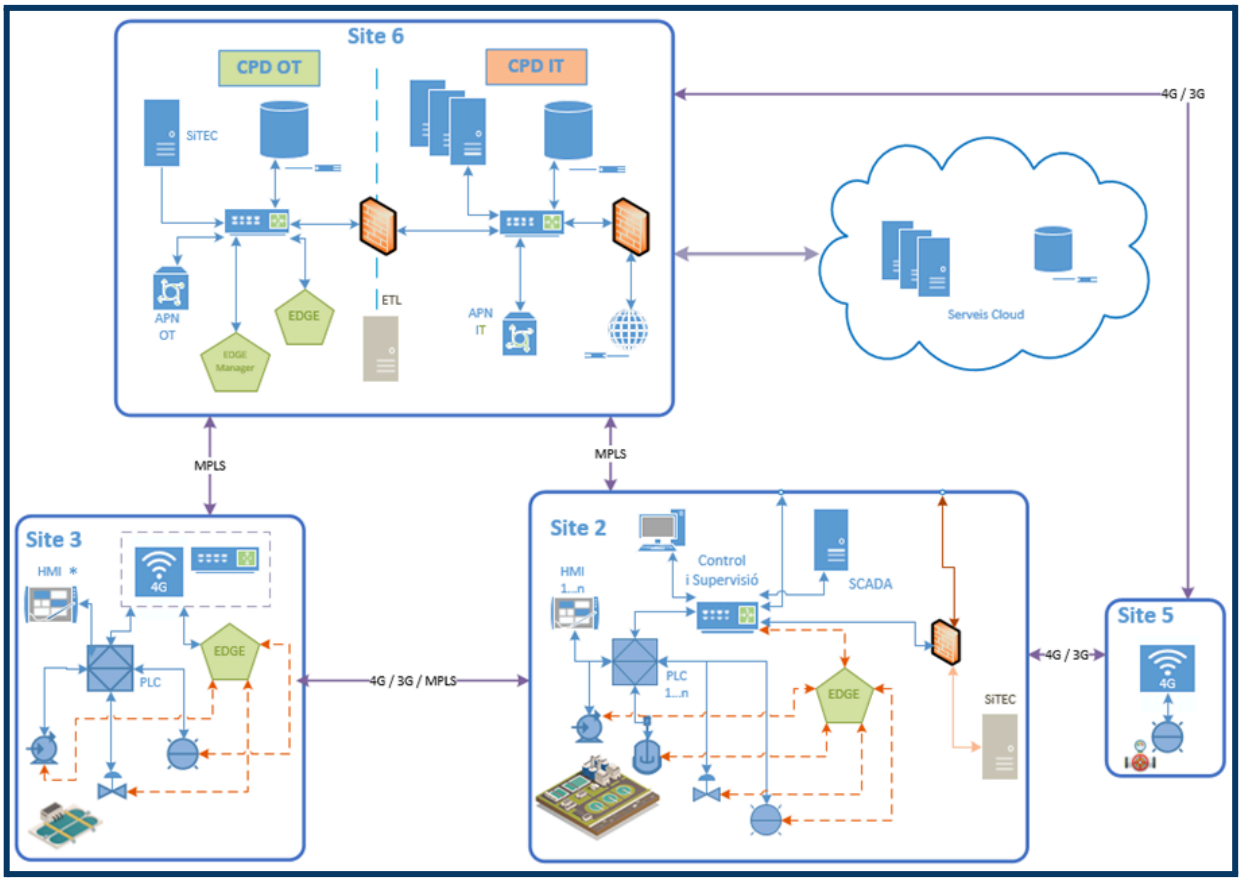


Figura 2. Distribución geográfica de la plataforma IIoT

5.2 Arquitectura por subsistemas

Una vez definidos los objetivos, necesidades y contexto de la iniciativa, y tras un análisis de alto nivel de las infraestructuras de comunicaciones y control industrial, y de la organización de estas dentro de la jerarquía de infraestructuras hidrológicas sobre las que se acometerá el proyecto, se ha realizado una primera clasificación de subsistemas necesarios, junto un esquema lógico que muestra a los mismos dentro del ecosistema de Aigües de Barcelona.

Se ha dividido el conjunto del sistema en 3 subsistemas independientes:

- Sistema de orquestación (morado).
- Sistema de ingesta (verde).
- Sistema de gobernanza del dato y plataforma de digitalización (naranja).

Dentro de los criterios de este diseño de alto nivel de la iniciativa, se ha marcado como esencial la independencia tecnológica de estos tres subsistemas, de modo que al mismo tiempo que puedan complementarse entre ellos, además de a otros subsistemas, presentes y futuros, dentro de las arquitecturas IT/OT de Aigües de Barcelona, puedan ser reemplazables sin que provoquen afectación alguna al resto de subsistemas. De este modo, podemos asegurar no solo el correcto diseño de la solución, sino su longevidad, esencial en entornos OT, a la vez que permitimos adaptar al mismo al estado del arte en cada una de las áreas técnicas.

El principal objetivo de este diseño es el despliegue de aplicaciones en las estaciones de forma rápida, sencilla y controlada. Una de estas aplicaciones, será el propio sistema de ingesta, transformación y transmisión de datos. Todos los datos son enviados al centro de control donde serán armonizados y estructurados para proporcionar un valor añadido a cada uno de estos datos obtenidos (optimización del proceso de producción, reducción de costes, medición de consumos energéticos, etc). Esto permite conseguir un modelo digital de las instalaciones de Aigües de Barcelona.

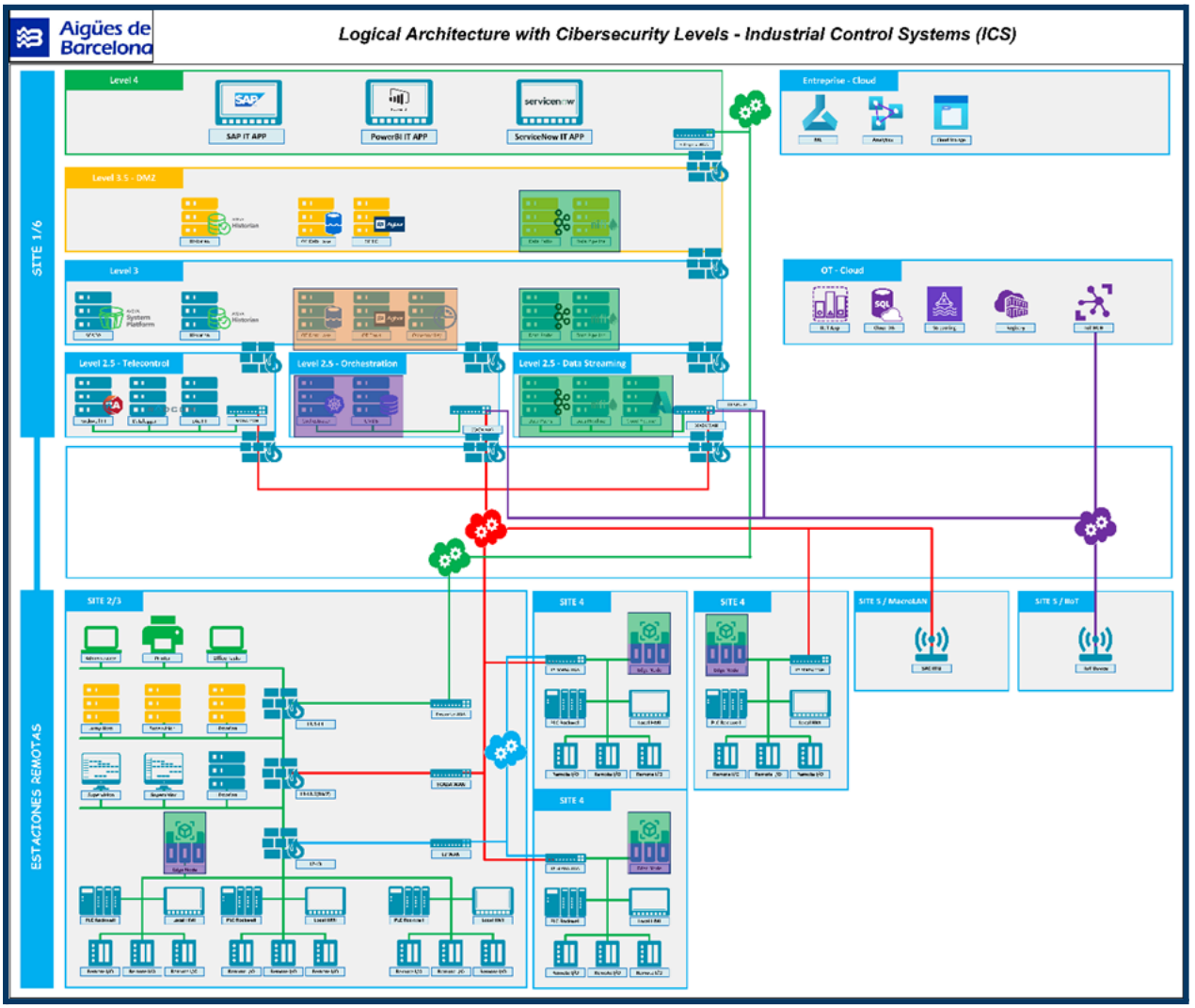


Figura 3. Arquitectura lógica con niveles de seguridad

5.2.1 Sistema de orquestación (morado)

El sistema de orquestación se encarga de gestionar el despliegue de aplicaciones en los diferentes nodos Edge localizados en las estaciones. Este sistema permite controlar qué herramientas se despliegan, cuando se despliegan y como se despliegan, lo cual impacta en tanto en el coste de mantenimiento, ya que evita realizar desplazamiento a las instalaciones en procesos de despliegues, como en la disponibilidad de las instalaciones al facilitar estos procesos.

Por otro lado, asegura el control de que el software desplegado es conocido y controlado de forma eficiente, en todo el ciclo de vida de este. Algunas de las herramientas que este tipo de sistemas nos ofrecen son:

- Gestión centralizada de equipos. Órdenes básicas como parar, reiniciar o arrancar la aplicación o el equipo Edge localizado en la estación remota.
- Monitorización del estado de cada Edge a través de diferentes métricas, como pueden ser el consumo de CPU o porcentaje de uso de RAM.
- Descarga y consulta de logs con diferentes niveles de severidad.

El sistema de orquestación se sitúa en una zona aislada para incrementar el nivel de seguridad de esta zona, ya que es el sistema encargado de gestionar el despliegue de las aplicaciones en los diferentes equipos de campo. En esta zona también se sitúa un CMDB (Configuration Management Data Base) en el que se almacenan las configuraciones de todos los equipos. El CMDB tiene una gran importancia para disponer de un recovery plan de todos los equipos que componen el sistema.

5.2.2 Sistema de ingesta (verde)

Sobre los nodos del sistema de orquestación (nodos Edge) correrá la aplicación que permite la comunicación con los equipos OT, la cual, mediante el uso de los diferentes protocolos comunes en ambientes industriales, obtendrá la información necesaria para las diferentes iniciativas de mantenimiento y explotación de las infraestructuras hidrológicas.

Esta misma herramienta es la encargada de la “limpieza” y estandarización de la información con el objetivo de que pueda ser consumida en “caliente”, es decir, es necesario que la herramienta sea capaz de armonizar la información evitando posteriores procesos de “limpieza” del dato que provocaría grandes latencias en procesos de ayuda a la decisión o en la aplicación de esta misma información en sistemas de “smart tuning” de procesos de regulación.

Toda la información recogida, podrá ser consumida de forma local, esto es, dentro del propio nodo Edge, al mismo tiempo que es enviada al centro de control o las áreas superiores de control dentro de la propia instalación para poder alimentar el resto de los consumidores, actuales o futuros.

Del mismo modo, es importante que el sistema permita la inclusión de nuevos “drivers” de comunicaciones que permitan la captación de información diversa.

El diseño indicado, hace que este sistema sea escalable ante el potencial crecimiento futuro de la infraestructura, sin detrimento de la operatividad de los elementos que la forman y garantizando la integridad operacional de las funcionalidades del sistema de supervisión.
Estos nodos Edge han sido situados en las redes locales de las estaciones para asegurar el tráfico de protocolos industriales no sale de la red local de las instalaciones.

La aplicación es altamente configurable y personalizable, con el objetivo de asegurar que es posible añadir nuevas variables o integrar nuevos equipos sin la necesidad de intervenciones complejas que puedan afectar al funcionamiento del sistema.

El valor bruto obtenido de los equipos localizados en la instalación puede ser transformado o sintetizado en función de los requerimientos de las aplicaciones utilizadas.

Los flujos de información, en especial aquellos que llegan al centro de control, son organizados mediante el uso de “brokers” de información, los cuales permiten generar flujos de diferentes características, atendiendo al tipo de consumo o necesidad de la aplicación.

Estos sistemas de flujos de datos sirven al mismo tiempo de fuente de la verdad, es decir, el sistema de orquestación de los flujos de datos permite el “reconsumo” de aquella información que quiera ser “reprocesada”.

Uno de los consumidores principales es las pipelines de datos, las cuales permiten configurar modificaciones, transformaciones, agrupaciones y reenvíos de la información nativa a otros sistemas, tanto a sistemas externos a la infraestructura de Aigües de Barcelona cuando se considere necesario como hacia sistemas localizados en las capas superiores de la infraestructura.

Como caso especial, se contempla el uso de una pipeline de datos hacia/desde sistemas Cloud, la cual se encarga de recoger o enviar datos desde/hacia soluciones de terceros que residan en nubes privadas de Aigües de Barcelona, o incluso que residan en nubes privadas de terceros. En el caso de que se quiera integrar una aplicación en el Cloud con inteligencia y servicios basados en el conocimiento, el Cloud Pipeline permite nutrir de los datos necesarios a esta aplicación externa para que los procese y genere los resultados. Este sistema también se encargaría de recibir y almacenar esos resultados.

Esta infraestructura tiene una réplica en el nivel superior con el fin de respetar los flujos de datos siguiendo la estructura de niveles definida y conseguir un aislamiento entre zonas.

5.2.3 Sistema de armonización y estructuración de datos (naranja)

Este sistema utiliza todos los datos subidos de las estaciones para organizar los activos de Aigües de Barcelona siguiendo el modelo de RAMI 4.0. Este modelo trata de establecer una organización de los activos industriales para la industria 4.0 organizada en 3 dimensiones.

El eje vertical define las propiedades de un sistema para realizar una representación virtual del mismo. Las capas de activos, integración y comunicación hacen referencia a los diferentes equipos de planta, así como la metodología de integración con los sistemas de control y la obtención de datos. Por ejemplo, se dispone de un caudalímetro (**asset**) integrado en un PLC a través de una conexión eléctrica de 4-20 mA (**integration**) del que se obtiene el dato a través de una comunicación Ethernet/IP (**communication**).

La capa de información incluye todos los datos obtenidos de los diferentes equipos de campo. Siguiendo el ejemplo anterior, qué datos se obtienen del caudalímetro (valor de caudal, unidades de medida, estado, etc).

La capa de Funcional aporta un significado a todos los datos obtenidos y la capa de negocio le añade el significado a nivel de negocio.

El eje de PROCESO aporta una visión global como sistema basado en la normativa IEC 62264. Esto aporta un gran valor en la definición del modelo digital ya que representa el sistema como

conjunto y no como elementos independientes. Es decir, en el anterior eje se mostraba una visión que representaba cada elemento de la instalación y en este eje se realiza una representación de la estación como sistema de producción.

El eje de PRODUCTO representa el ciclo de vida de las instalaciones y los productos basado en la normativa IEC62890. Representa la vida útil del activo, desde el desarrollo hasta la eliminación. Por lo tanto, es la gestión del ciclo de vida para sistemas y productos, utilizada en la medición, el control y la automatización de procesos industriales.

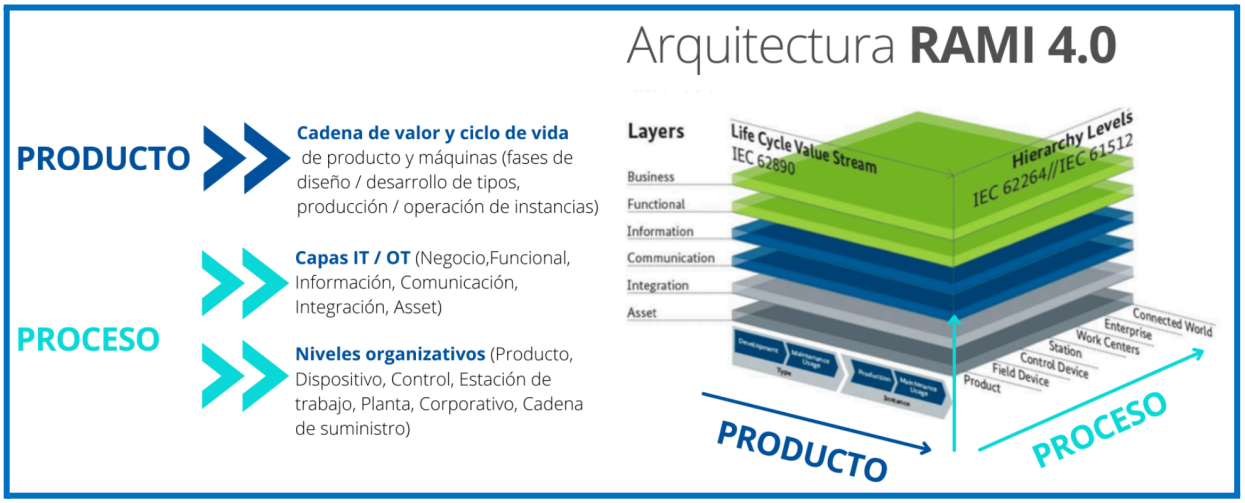


Figura 4. Modelo arquitectura Reference Architecture Model Industrie 4.0 (RAMI 4.0)

Este modelo aporta las siguientes ventajas:

- El modelo RAMI 4.0 integra diferentes perspectivas de los usuarios.
- Proporciona una forma común de ver las tecnologías de la industria 4.0.
- Aporta un entendimiento común para las normas y los casos de uso.
- El modelo considera un mapa de soluciones de la industria 4.0.
- Está orientado para trazar los requisitos de los sectores junto con las normativas nacionales e internacionales para definir y seguir desarrollando la Industria 4.0.

6 REQUERIMIENTOS TÉCNICOS DE EJECUCIÓN

6.1 Lote 1: Requerimientos técnicos ámbito SCI-OT

6.1.1 Hardware del sistema: Industrial PC

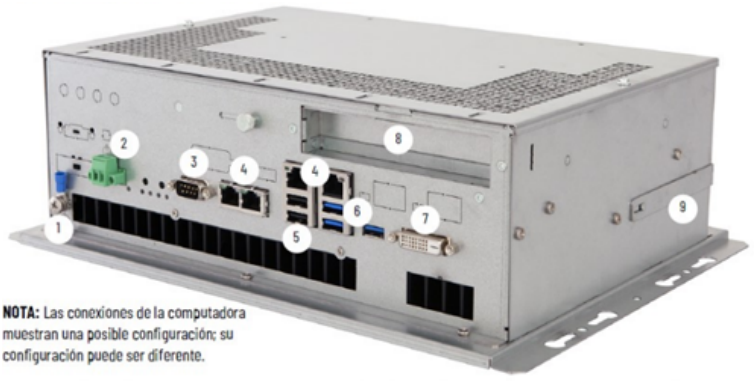
Se contempla que el dispositivo de ingesta tenga las capacidades de ejecutar aplicaciones que realicen un procesado de datos de forma local. El hardware necesario para realizar la ingesta de datos se localizará en los emplazamientos:

- EDAR Baix Llobregat
- EDAR Sant Feliu
- EDAR Gavá
- EDAR Besós
- EDAR Montcada

El Edge instalado en estos emplazamientos se encargará de recolectar toda la información de esa estación y de las estaciones dependientes.

El Edge debe garantizar la eficacia y eficiencia tanto en la ingesta de datos como su posible tratamiento en las plantas de Aigües de Barcelona, por ello se define a continuación un equipo Edge con las especificaciones mínimas.

A modo de ejemplo se presenta un equipo básico como el PC de Rockwell modelo 6300B-PBCDNB-5DCBNNNNNNCNN-NN1S, el cual cuenta con una amplia variedad de características que lo hacen idóneo para cumplir con todas las necesidades definidas.



NOTA: Las conexiones de la computadora muestran una posible configuración; su configuración puede ser diferente.

N.º	Descripción
1	Tornillo de puesta a tierra
2	Conexión de alimentación eléctrica de entrada de CC
3	Puerto serial RS-232 (DB9M)
4	4 puertos Ethernet LAN, RJ45
5	2 puertos USB 2.0, tipo A

N.º	Descripción
6	3 puertos USB 3.0, tipo A
7	Puerto DVI-D, Full HD
8	4 ranuras expansoras PCIe
9	Ranura de tarjeta CFast

Ilustración 1: Modelo equipos EDGE

En términos generales, el PC de Rockwell modelo 6300B tiene un montaje específico para entornos industriales, con una alimentación eléctrica aislada de 24 VDC y diseño sin ventilador,

lo que garantiza una mayor eficiencia y durabilidad del equipo. Tiene una ranura PCI/PCIe para expansiones y se basa en el procesador Intel Core i5.

El equipo tiene una memoria de 16 GB RAM, lo que significa que puede manejar grandes cantidades de datos de manera fluida y sin comprometer el rendimiento en las tareas de ingesta de datos. Cuenta con una unidad de almacenamiento SSD de 512GB 2.5 SSD1, lo que garantiza una gran capacidad de almacenamiento y acceso rápido a los datos. El ítem 1 del presupuesto hace referencia al hardware descrito o de características similares *(1.Suministro HW - Edge - Celeron 4C/4T - 16GB RAM - 512GB SSD).*

El PC de Rockwell indicado arriba no viene con ningún software de automatización de Rockwell preinstalado. Sin embargo, cuenta con garantía branding estándar de la marca. El ítem 2 del presupuesto hace referencia a todo el software necesario a ser instalado en el EDGE con la finalidad de la ingesta de datos *(2. Suministro SW - Licencias - IIoT Data Adquisition System / anual)*.

En definitiva, el equipo Edge seleccionado para la ingesta de datos en las plantas de Aigües de Barcelona es el PC de Rockwell modelo 6300B-PBCDNB-5DCBNNNNNNCNN-NN1S o equivalente, con gran capacidad de procesamiento, almacenamiento y eficiencia energética, lo que garantiza una eficaz y eficiente ingesta de datos en las plantas integradas en la plataforma de IoT.

A continuación, se muestra el equipo seleccionado:

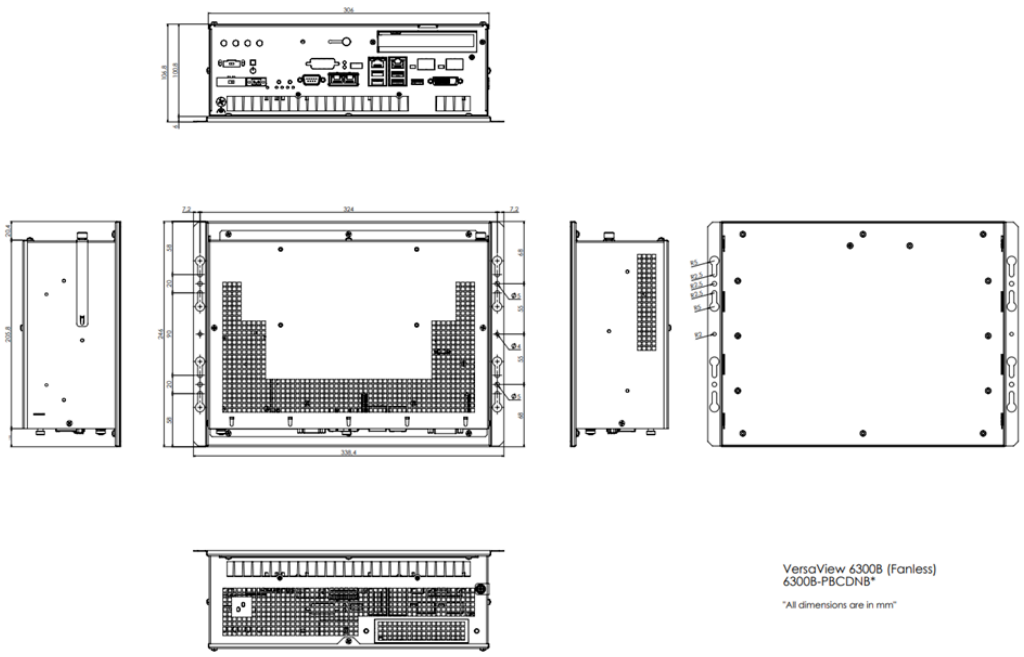


Ilustración 2: Dimensiones equipos EDGE

El equipo Edge descrito en los apartados anteriores (o equivalente) se instalará en cada una de las ubicaciones en una caja Schneider modelo NSYCRN108300 de 1000*800*300mm o equivalente con puerta plena. La caja cuenta con un sistema de sellado eficiente que evita la

entrada de polvo y otros contaminantes ambientales en su interior. De esta manera, se asegura que el equipo Edge instalado en su interior estará protegido ante posibles fallos o daños producidos por la exposición a factores ambientales adversos.

Ilustración 3: Ejemplo diseño caja externo e interno

Para ofrecer la máxima fiabilidad y continuidad en el suministro eléctrico se incorpora una alimentación redundante que garantiza la alimentación del sistema. Se compone de un UPS (Sistema de Alimentación Ininterrumpida) de la marca PHOENIX CONTACT o equivalente, con una capacidad de 24V y 38Ah. El UPS ofrece información sobre su estado a través de protocolos estándar industriales. Esto se traduce en una mayor capacidad de control y diagnóstico del estado del sistema, permitiendo tomar medidas preventivas antes de que ocurran posibles fallos. A continuación, se muestra un esquema genérico del sistema descrito.

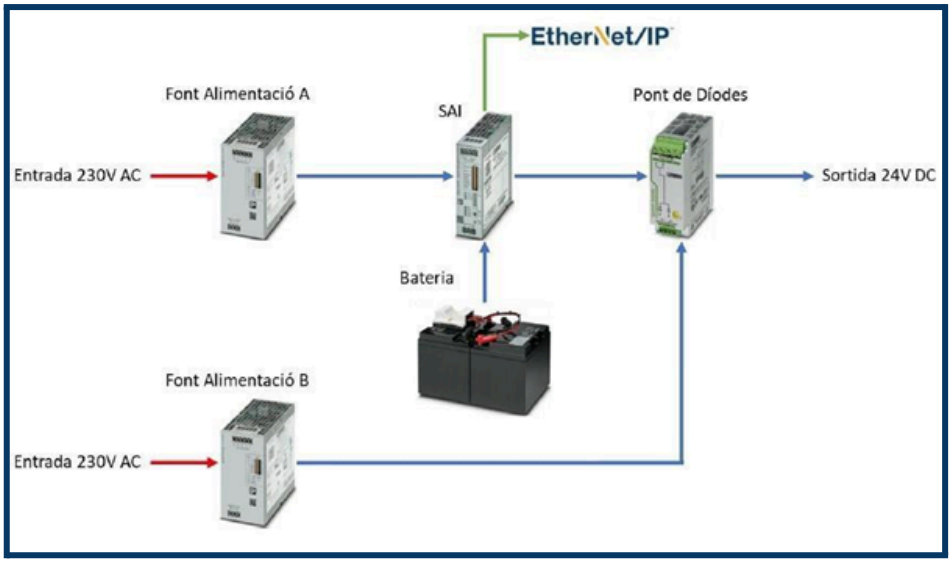


Ilustración 4: Esquema genérico de instalación

En cada una de las ubicaciones se localiza un Edge situado en una caja independiente tal y como se ha explicado anteriormente. A continuación, se elabora un listado completo de todos los materiales que se instalarán en cada una de las ubicaciones. El ítem 3 del presupuesto hace referencia al pequeño material contemplando para la instalación de dichos EDGE *(3. instalación y PeM - Edge - Incluye pequeño material eléctrico para la adaptación al armario industrial)*.

Cantidad	Descripción
1	Armario metálico marca Schneider mod. NSYCRN108300 de 1000*800*300 mm. con puerta plena o equivalente.
1	A9R81240 Diferenciales SCHNEIDER iID 40/2/30 mA o equivalente.
2	Magnetotérmicos SCHNEIDER iC60H C Pcc.10KA de 16 A II, ref. A9F89216 (Fuentes de alimentación) o equivalente.
1	A9F89206 Magnetotérmicos SCHNEIDER iC60H C Pcc.10KA de 6 A II (ventilación cuadro) o equivalente.
1	Magnetotérmicos SCHNEIDER CC C60H-DC C Pcc.10KA de 20 A II, ref. A9N61532 o equivalente.
1	Termostato doble 1NA/NC 0-60ºC SCHNEIDER Ref. NSYCCOTHD o equivalente.
1	Ventilador 38m3/h 230Vca 137x117mm SCHNEIDER Ref. NSYCVF38M230PF o equivalente.
1	Rejilla y filtro de salida SCHNEIDER mod. NSYCAG92LPF+NSYCAF92 de 125x125 o equivalente.
2	Fuente alimentacion Phoenix Quint-PS 1AC 24Vdc de 20A ref. 2904602 o equivalente.
1	Interface comunicación Phoenix RJ45 24Vdc 20A. ref. 2907074 o equivalente.
1	Modulo diodo Phoenix 12-24Vcc 2*20A redundancia ref. 2320157 equivalente.
1	2320335 módulo Energía PHOENIX CONTACT tipo UPSBAT/ VRLA/24DC/38AH ref, 24 V DC, 38 Ah o equivalente.
1	2320458 Set mont. battery mounting case fij. bat. PHOENIX o equivalente.
1	Montaje de PC Rockwell tipo 6300B-PBCx o equivalente.
1	6300B-PBCDNB-5DCBNNNNNNCNN-NN1S o equipo equivalente.

La caja del Edge será instalada en las ubicaciones definidas por el personal de Aigües de Barcelona, además también se realizará la alimentación a través de una acometida de 230V con una sección de 3*4 mm2. La previsión es que la distancia desde el armario más cercano hasta la caja eléctrica no sea mayor a 15 metros, y que la conexión se realice a través de canales existentes.

Para proteger la acometida, se suministra e instala un equipo de protección en el cuadro existente. Esta protección debe estar formada por un magnetotérmico de la marca SCHNEIDER iC60H Pcc.10KA de 20A II con referencia A9F89220 y un cableado del interior y bornes.

Una vez que la caja eléctrica esté instalada y alimentada, la conexión a la red OT se realizará a través de dos cables Ethernet en el switch de la red OT más cercano a la caja (uno para el Edge y otro para el SAI).

Es importante destacar que se realizarán los planos eléctricos de todas las cajas instaladas en formato EPLAN. Estos planos deben ser proporcionados en formato pdf y formato editable. Además, se incluirá una copia física de los planos eléctricos en cada una de las ubicaciones con el

fin de facilitar el mantenimiento. Todos los planos deben cumplir con las normas y regulaciones aplicables.

En resumen, para instalar correctamente la caja eléctrica, se debe garantizar su alimentación eléctrica, proteger la acometida con un equipo de protección, conectar la caja a la red OT mediante dos cables Ethernet, y proporcionar planos eléctricos en EPLAN para su instalación. Todo esto se realizará de acuerdo con las normas y regulaciones aplicables.

Tras la instalación de la caja, se emitirá un informe que incluirá evidencias de que todos los puntos anteriores han sido cumplidos acorde a las especificaciones.

6.1.2 Sistema de orquestación (RFO)

Se deberá suministrar y configurar un sistema de orquestación con todo el software y el hardware necesario atendiendo a los requerimientos funcionales y de diseño descritos a continuación, el ítem 6 del presupuesto hace referencia al soporte del sistema de orquestación en régimen de 8x5x12 *(6. Suministro SW - Licencias Orquestador - Orquestador Industrial (Soporte 8x5 - <12 horas)*, el ítem a las licencias que se instalarán en cada uno de los 5 EDGE (*7. Suministro SW - Licencias Orquestador - Orquestador Industrial - New Node)* y el ítem 8 a los trabajos de instalación y puesta en marcha de todo el sistema de orquestación *(8. Instalación y PeM - Edge - Instalación y configuración de nodos de Orquestación).*

El sistema de orquestación se encargará de gestionar el despliegue de aplicaciones en los diferentes nodos Edge localizados en las estaciones. Este sistema permitirá controlar qué herramientas se despliegan, cuando se despliegan y como se despliegan, lo cual impacta tanto en el coste de mantenimiento, ya que evita realizar desplazamientos a las instalaciones en procesos de despliegues, como en la disponibilidad de las instalaciones al facilitar estos procesos.

Por otro lado, asegura el control de que el software desplegado es conocido y controlado de forma eficiente, en todo el ciclo de vida de este. Algunas de las herramientas que este tipo de sistemas nos ofrecen son:

- Gestión centralizada de equipos. Órdenes básicas como parar, reiniciar o arrancar la aplicación o el equipo Edge localizado en la estación remota.
- Monitorización del estado de cada Edge a través de diferentes métricas, como pueden ser el consumo de CPU o porcentaje de uso de RAM.
- Descarga y consulta de logs con diferentes niveles de severidad.

El sistema de orquestación se sitúa en una zona aislada para incrementar el nivel de seguridad de esta zona, ya que es el sistema encargado de gestionar el despliegue de las aplicaciones en los diferentes equipos de campo. En esta zona también se sitúa un CMDB (Configuration Management Data Base) en el que se almacenan las configuraciones de todos los equipos. El CMDB tiene una gran importancia para disponer de un plan de recuperación de todos los equipos que componen el sistema. El ítem 4 del presupuesto hace referencia a los trabajos de "enrolado" de todos los nodos EDGE en dicha plataforma de orquestación *(4. Instalación y PeM - Edge - Enroll de nodo Edge en IIoT Digitalization Platform y Orquestador Industrial).*

Como requisitos funcionales de la aplicación de orquestación (RFO) se marcan:

RFO-001: Plataforma única donde gestionar nodos Edge

Capacidad de gestión de PC's industriales desde plataforma central. Existe mucha confusión respecto al Edge computing. Muchas veces los fabricantes de hardware utilizan este concepto para definir simplemente los ordenadores industriales. No obstante, para considerar que una solución es de Edge computing, es necesario poder gestionar los nodos (ordenadores industriales) desde una plataforma central.

RFO-002: Agnóstico al Hardware
Es necesario que se puedan gestionar todo tipo de PC's industriales, de cualquier fabricante, que soporten los procesadores ARM, Intel o AMD. Una plataforma que gestione nodos Edge de un solo fabricante, no puede calificarse de solución Edge, sino plataforma de gestión de una marca. Para ser considerada plataforma Edge computing, es necesario que ésta sea agnóstica al hardware y pueda funcionar con dispositivos de diversos fabricantes, desde pequeños PC's industriales, a grandes servidores.

RFO-003: Gestión de dispositivos sin necesidad de VPN
Todos los nodos pueden ser gestionados y controlados, de forma segura, desde una plataforma centralizada, sin necesidad de crear VPN para cada uno de los nodos. Los equipos tienen que ser gestionados sin necesidad de crear VPN con cada uno de ellos, pero manteniendo el máximo nivel de seguridad. Todas las conexiones tienen que ser mediante MQTTS, con certificados únicos para cada dispositivo.

RFO-004: Gestión ciclo de vida de OS
El OS tiene que ser actualizado también desde la plataforma de Edge Computing. El OS es una parte crítica de la solución de Edge computing, por lo que es necesario mantener todo su ciclo de vida con las mismas facilidades que el resto de las aplicaciones.

RFO-005: Soporte GPU
Poder soportar hardware con GPU (Graphics Processing Unit) para despliegue de aplicaciones de IA. Soportar GPU de los PC's industriales puede tener grandes ventajas, sobre todo en aplicaciones de visión artificial. Por tanto, una solución Edge debe poder soportar el uso de GPU para este tipo de aplicaciones.

RFO-006: Orquestación aplicaciones nativas
Posibilidad de desplegar aplicaciones nativas sobre los nodos Edge. Esto es una gran ventaja porque las aplicaciones nativas son muy eficientes.

RFO-007: Orquestación aplicaciones docker
Posibilidad de desplegar aplicaciones en formato docker en los nodos. Docker se ha convertido en un estándar, por lo que es una gran ventaja poder desplegar dockers en todos los nodos de forma centralizada.

RFO-008: Disponibilidad de conectores industriales
Disponer de librería de conectores industriales, principalmente OPC UA y MODBUS. Una solución de Edge computing debe también ofrecer una librería de conectores industriales con otros dispositivos, utilizando los protocolos más comunes del mercado, entre ellos OPC UA y MODBUS.

RFO-009: Plataforma despliegue Machine Learning
Facilidad para desplegar algoritmos de Machine Learning fácilmente en los nodos. Posibilidad de que se puedan desplegar algoritmos de ML en los nodos, actuando sobre los dispositivos conectados si fuera necesario.

RFO-010: Opción MLOps en el nodo
Aprendizaje de ML en los nodos Edge. El nodo Edge debe disponer de mecanismos para desplegar aplicaciones de aprendizaje y Machine Learning Operations en los propios nodos, para facilitar el despliegue de aplicaciones inteligencia artificial en entornos seguros donde no se puedan transmitir muchos datos.

RFO-011: Operaciones por lotes
Poder desplegar aplicaciones o gestionar nodos en lote para simplificar la gestión. A la hora de gestionar miles de dispositivos desplegados en campo es crucial poder operarlos en paralelo, mediante comandos en lote. Pero la potencia que ofrece un comando aplicado a miles de dispositivos también conlleva una gran responsabilidad. Por ello, es necesario previsualizar las acciones que se van a ejecutar, simular los resultados antes de ejecutar la acción y restringir estas acciones a usuarios con permisos suficientes para llevarlas a cabo.

RFO-012: Telemetría de nodos Edge
Monitoriza la salud del Edge y adelántate a los problemas para garantizar la continuidad del sistema. Comprobación en tiempo real parámetros básicos del rendimiento de los nodos tales como el uso de CPU, memoria RAM, temperatura, etc.

RFO-013: Data Analytics
Posibilidad de visualizar datos directamente en los nodos. Es importante poder decidir si la información capturada, y almacenada en el nodo, puede ser accesible, visualizada y analizada en el propio nodo, o enviada a un servidor central.

RFO-014: Opción plataforma Cloud / On Premises
La plataforma de gestión de nodos Edge debe poder estar disponible en la nube o instalarse on site en caso de ser requerido. La plataforma de Edge Computing estará preferiblemente accesible en la nube y estará siempre actualizada. No obstante, también deberá poder ser instalada on-premise en el datacenter del cliente si fuera requerido, idealmente utilizando microservicios.

RFO-015: VPN para datos
Opción de crear canales VPN para el plano de usuario. Aunque los dispositivos tienen que ser gestionados sin necesidad de VPN, la plataforma debe de disponer de una funcionalidad de VPN para poder conectarse en remoto a los datos desde fuera de la red privada donde se encuentra el nodo.

RFO-016: Nodos Edge bastionados
Dispositivos securizados en profundidad sin acceso de usuario/pass, puertos cerrados, sin canales de comunicación entrantes y canales salientes seguros. Importante que los dispositivos Edge no sean accesibles mediante interfaces de entrada como pantallas o teclados. No tienen que existir puertos abiertos ya que todas las comunicaciones tienen que ser de salida.

RFO-017: Encriptación de datos
Todos los datos del usuario almacenados en el dispositivo, ya sea en funcionamiento o apagado, o enviados a través de cualquier red, están encriptados con los estándares de la industria. Protección ante alteración de datos en el tránsito de red asegurando la integridad de estos.

RFO-018: Certificado único por dispositivo

La autenticación y autorización de cada uno de los nodos está asegurada por certificados criptográficos únicos. Identificación única de equipos que evita amenazas de suplantación.

RFO-019: Sistema de aprovisionamiento seguro
Primera secuencia de arranque segura en la que se configura tanto el estado inicial del dispositivo como sus certificados de comunicación finales. Mejora significativamente la seguridad, la confiabilidad, la facilidad de uso y el cumplimiento normativo de los dispositivos Edge.

RFO-020: Arranque seguro
Arranque de los nodos con firmware de confianza. Realización de una serie de algoritmos criptográficos en el arranque para garantizar que el software no ha sido modificado por terceros. Se reduce el riesgo de que el dispositivo sea comprometido por atacantes malintencionados. También se mejora la confiabilidad del dispositivo y el riesgo de errores.

RFO-021: Soporte TPM
Verificación de las firmas del firmware con los certificados o claves de cifrado almacenados en el TPM (Trusted Platform Module). Garantiza que únicamente se carga en los equipos el firmware auténtico y no modificado.

RFO-022: Integridad del sistema
Mantenimiento preventivo de seguridad. Supervisión de los errores y los eventos no deseados, lo que le permite analizar e identificar posibles ataques y eventos relacionados con la seguridad y llevar a cabo un mantenimiento preventivo

RFO-023: Soberanía de los datos
Separación de los planos de control y de usuario. La plataforma Edge no debe poder acceder a los datos de usuario, por lo que el cliente debe mantener la plena propiedad del sistema.

6.1.3 Sistema de ingesta (RSI)

Se deberá suministrar un sistema de ingesta de datos y configurar el mismo con toda la información adquirida a través de la sensórica instalada en las actuaciones A6 y A8 (ver anexo 3).

Requisitos funcionales del sistema de ingesta (RSI). Funciones y características mínimas que debe cumplir el sistema de ingesta para conseguir los objetivos y necesidades. Requisitos específicos, medibles y verificables:

RSI-01: Capacidad de distribución
El sistema de ingesta debe ser capaz de distribuirse en múltiples nodos de forma independiente, lo que permite que cada componente del sistema tenga su propio entorno y recursos aislados.

RSI-02: Capacidad standalone
La aplicación debe contar con la capacidad de permitir que los nodos que estén leyendo datos de los equipos OT sigan funcionando incluso en caso de perder la conexión con el servidor centralizado.

RSI-03: Capacidad de reenvío tras recuperación

El sistema de ingesta debe ser capaz de almacenar temporalmente los datos recopilados en cada uno de sus nodos, hasta que se restablezca la conexión de estos nodos con el servidor y se pueda realizar la transferencia de datos.

RSI-04: Identificador único
Todos los nodos deben contar con un identificador único que permita su identificación en el sistema. Este identificador debe ser único en todo el sistema y debe ser asignado de forma automática por la aplicación en el momento de su despliegue. El identificador debe ser utilizado para garantizar la seguridad de la información, evitando suplantaciones de identidad y permitiendo la trazabilidad de los datos recibidos y enviados por cada nodo.

RSI-05: Capacidad de ser dockerizable
El sistema de ingesta debe tener la capacidad de ser dockerizada.

RSI-06: Capacidad de ser desplegado mediante orquestadores
El sistema de ingesta debe tener la capacidad de ser desplegable mediante orquestadores de contenedores. Esto permitirá que el despliegue y mantenimiento de la plataforma se automatice, lo que reducirá el tiempo y esfuerzo necesarios para administrar y recuperar ante fallos la plataforma.

RSI-07: Procesamiento de datos
El sistema de ingesta debe ser capaz de procesar más de 1000 mensajes por segundo, lo que implica una capacidad de procesamiento significativa.

RSI-08: Lógica de alertas
El sistema de ingesta debe permitir añadir lógica para generar alertas en caso de que se detecten problemas o eventos específicos.

RSI-09: API para extensibilidad de plataforma
El sistema de ingesta debe contar con una API bien definida que permita a los usuarios extender su funcionalidad. La API debe ser fácil de usar y bien documentada para que los usuarios puedan desarrollar y agregar funcionalidades no existentes en la solución.

RSI-10: Soporte para protocolos OT Modbus
La aplicación debe ser capaz de recoger datos de los sensores o actuadores y autómatas de las estaciones en el protocolo OT (Operational Technology) Modbus. La aplicación debe ser capaz de integrarse con este protocolo para recolectar, analizar y procesar los datos en tiempo real. Además, la aplicación debe ser capaz de detectar y solucionar errores en la comunicación con estos dispositivos, así como de recuperarse de forma automática ante posibles fallos. La configuración de los dispositivos debe ser fácilmente editable y la aplicación debe ser capaz de reconocer los cambios en la configuración de forma dinámica.

RSI-11: Soporte para protocolos OT TCP/IP
La aplicación debe ser capaz de recoger datos de los sensores o actuadores y autómatas de las estaciones en el protocolo OT (Operational Technology) TCP/IP. La aplicación debe ser capaz de integrarse con este protocolo para recolectar, analizar y procesar los datos en tiempo real. Además, la aplicación debe ser capaz de detectar y solucionar errores en la comunicación con estos dispositivos, así como de recuperarse de forma automática ante posibles fallos. La configuración de los dispositivos debe ser fácilmente editable y la aplicación debe ser capaz de reconocer los cambios en la configuración de forma dinámica.

RSI-12: Soporte para protocolos OT OPC UA

La aplicación debe ser capaz de recoger datos de los sensores o actuadores y autómatas de las estaciones en el protocolo OT (Operational Technology) OPC UA. La aplicación debe ser capaz de integrarse con este protocolo para recolectar, analizar y procesar los datos en tiempo real. Además, la aplicación debe ser capaz de detectar y solucionar errores en la comunicación con estos dispositivos, así como de recuperarse de forma automática ante posibles fallos. La configuración de los dispositivos debe ser fácilmente editable y la aplicación debe ser capaz de reconocer los cambios en la configuración de forma dinámica.

RSI-13: Soporte para protocolos OT BACnet
La aplicación debe ser capaz de recoger datos de los sensores o actuadores y autómatas de las estaciones en el protocolo OT (Operational Technology) BACnet. La aplicación debe ser capaz de integrarse con este protocolo para recolectar, analizar y procesar los datos en tiempo real. Además, la aplicación debe ser capaz de detectar y solucionar errores en la comunicación con estos dispositivos, así como de recuperarse de forma automática ante posibles fallos. La configuración de los dispositivos debe ser fácilmente editable y la aplicación debe ser capaz de reconocer los cambios en la configuración de forma dinámica.

RSI-14: Personalización de señales
La aplicación debe permitir la personalización del detalle de cada una de las señales recibidas, incluyendo el nombre de la señal, su unidad de medida, su rango de valores esperados y otros atributos relevantes.

RSI-15: Representación de la calidad del dato
La aplicación debe ser capaz de representar la calidad del dato de cada señal, utilizando indicadores como el porcentaje de validez, la precisión, entre otros.

RSI-16: Representación concisa
La representación de los datos debe ser clara y fácilmente interpretable, permitiendo a los usuarios identificar posibles problemas o anomalías de forma rápida y eficiente.

RSI-17: Capacidad de ser configurable
La configuración de los equipos y señales debe ser fácilmente editable.

RSI-18: Reconocimiento ante cambios de configuración
La aplicación debe ser capaz de reconocer los cambios en la configuración de forma dinámica.

RSI-19: Personalización de representación
La representación del detalle de los equipos monitorizados en las estaciones debe ser personalizable.

RSI-20: Detección de fallos
La aplicación debe permitir a los usuarios identificar posibles problemas o anomalías de forma rápida y eficiente.

RSI-21: Funcionalidad de búsqueda
El sistema de ingesta debe contar con un buscador que permita a los usuarios encontrar información de forma rápida y sencilla. El buscador debe ser capaz de realizar búsquedas por diferentes criterios, como el nombre del equipo, el tipo de señal, el nombre del usuario, entre otros.

RSI-22: Funcionalidad segmentación de usuarios
La aplicación debe permitir la segmentación de roles y permisos de los usuarios: La aplicación debe ser capaz de asignar diferentes roles y permisos a los usuarios, de manera que cada usuario tenga acceso solo a las funcionalidades y datos que le correspondan. Los roles y permisos deben ser definidos por los administradores del sistema y deben poder ser modificados en cualquier momento.

RSI-23: Funcionalidad gestión de usuarios
La gestión de usuarios debe ser fácil y permitir la creación, modificación y eliminación de usuarios de forma sencilla y segura: La aplicación debe permitir a los administradores del sistema la creación, modificación y eliminación de usuarios de forma sencilla y segura. Los usuarios deben ser autenticados antes de poder acceder a la aplicación y deben ser identificados por un nombre de usuario y una contraseña segura.

RSI-24: Funcionalidad auditoria de usuarios
La aplicación debe ser capaz de registrar las acciones realizadas por cada usuario, así como la hora y fecha en que se realizaron. Esta información debe ser fácilmente accesible por los administradores del sistema, permitiendo la identificación de posibles problemas o vulnerabilidades.

RSI-25: Funcionalidad de segmentación de roles
La aplicación debe permitir la configuración de roles y permisos de forma granular, de manera que los administradores del sistema puedan asignar permisos específicos a cada usuario. Esto permitirá un mayor control y seguridad de los datos y funcionalidades de la aplicación.

RSI-26: Funcionalidad seguridad de usuarios
La aplicación debe ser capaz de notificar a los administradores del sistema sobre posibles violaciones de seguridad, como intentos de acceso no autorizados o cambios en la configuración de roles y permisos.

6.1.4 Plataforma de IIoT (RO)

Se deberá suministrar, instalar, configurar y programar una plataforma que permita:

- La captación de información (a través del SW de ingesta)
    - Integración con otras soluciones/herramientas del negocio (ERP, GMAO, LIMS, CRM,…)
- La contextualización de la información, incluyendo datos provenientes de la ingesta, pero también información adicional (fabricante, datos de fabricante, datos nominales de funcionamiento, etc.)
    - Además la principal funcionalidad es la de parametrizar activos y crear plantillas, para una mejor actuación y despliegue de casos de uso y analítica. (Things and Shapes).
- Capa analítica. Fundamentalmente es donde se desarrollan los casos de uso específico.
    - Analítica descriptiva: para casos típicos de monitorización y seguimiento de KPIs (Rendimiento de bombas, OEE, cálculos, conteo de horas efectivas de funcionamiento,…)
    - Analítica avanzada: creación, gestión y monitorización de algoritmos de analítica avanzada para la resolución de casos específicos (detección de anomalías, análisis multivariable, predictividad a la salida de un proceso (mantenimiento, calidad, etc).
- Orquestación. Capa para automatizar flujos de trabajo.
    - Gracias a la integración con otras herramientas de negocio (ERP, GMAO, etc.) se pueden crear reglas de negocio para automatizar ciertas funciones.
        - Notificación via email/IM/… de un determinado situación
        - Generación de flujo de trabajo a través de una herramienta como:
            - Creación de una OT en un GMAO o similar.

    - Solicitar una orden de compra en un ERP o similar.
    - …
- Visualización. La capa de visualización donde los usuarios son capaces de ver la información relevante para su negocio/estación/activos de manera personalizada.

Más concretamente los requisitos de la plataforma, herramientas y prácticas que permiten monitorizar y analizar el rendimiento y el estado de los dispositivos y servicios en tiempo real, con el objetivo de detectar, diagnosticar y solucionar problemas en la plataforma y mejorar su eficiencia y calidad son:

RO-01: Gestión de gráficos (zoom)
El sistema de observabilidad debe ser capaz de hacer zoom sobre los gráficos históricos para poder enfocarse en un periodo de tiempo específico.

RO-02: Gestión de gráficos (desplazamiento sobre el eje temporal)
El sistema de observabilidad debe tener la capacidad de poder desplazarse por el eje temporal de los gráficos donde se representan los datos históricos.

RO-03: Gestión de gráficos (representar varias señales)
El sistema de observabilidad debe de tener la capacidad de graficar varias señales a la vez.

RO-04: Compatibilidad con herramientas de monitoreo
La aplicación debe ser compatible con herramientas estándar de monitoreo, como Nagios, Zabbix o Prometheus, para permitir una fácil integración con sistemas existentes.

RO-05: Representación de gráficos
El sistema de observabilidad debe contar con la capacidad de representación de datos históricos mediante gráficos para así facilitar la visualización y análisis de estos datos.

RO-06: Creación de dashboards
El sistema de observabilidad debe permitir a los usuarios ser capaces de generar sus propios dashboards personalizados para visualizar los datos de manera específica.

RO-07: Compartir dashboards
El sistema de observabilidad debe permitir que los dashboards puedan ser compartidos entre usuarios del mismo grupo para permitir una fácil colaboración.

RO-08: Segmentación de organizaciones
El componente de observabilidad de la aplicación debe permitir organizar la información en diferentes organizaciones o grupos para una gestión más eficiente.

RO-09: Estándar de monitoreo
La aplicación debe ser capaz de soportar la monitorización de máquinas Linux y Windows a través de protocolos estándar como SNMP o WMI.

RO-10: Estándar de los canales de comunicación
Los canales de comunicación de la aplicación deben ser monitorizables a través de un estándar como syslog para una fácil detección de errores y problemas.

RO-11: Lógica de alertas

El sistema de observabilidad debe de poder permitir añadir lógica para generar alertas en caso de que se detecten problemas o eventos específicos.

RO-12: Monitoreo mediante REST API
Todos los componentes del sistema deben contar con una REST API para exponer el estado y las métricas de los diferentes componentes que conforman la solución. Esta API debe permitir la monitorización remota y en tiempo real de los componentes, facilitando la detección y el diagnóstico de problemas

RO-13: Integración REST API
La plataforma debe permitir el uso de REST API para realizar la integración de la información de todos los sistemas externos que componen la infraestructura IIoT (estado de los Edge, pipelines, data paths…).

RO-14: Monitorización infraestructura IIoT
La plataforma debe realizar la monitorización de todos los módulos que componen la infraestructura IIoT notificando de todos los comportamientos anómalos del sistema.

RO-15: Gestión centralizada de logs
La aplicación debe ser capaz de enviar sus logs a un sitio centralizado para su análisis y gestión.

RO-16: Visión histórica de logs
El sitio centralizado debe permitir la visualización de los logs en una línea temporal.

RO-17: Búsqueda de logs
El sitio centralizado debe permitir la búsqueda de logs por tipo de evento, timestamp y otros parámetros relevantes.

RO-18: Contenido del log
Los logs del sistema de observabilidad deben contener información precisa, incluyendo hora de registro, gravedad del evento, origen del evento y una descripción detallada del mismo.

RO-19: Seguridad de envio de logs
La aplicación debe enviar los logs de forma segura, utilizando técnicas de encriptación y autenticación para garantizar la integridad y confidencialidad de los datos.

RO-20: Almacenamiento de logs
Los logs del sistema de observabilidad deben ser almacenados de forma segura y protegidos contra pérdidas de datos.

RO-21: Alerta mediante logs
La aplicación debe ser capaz de generar alertas en caso de que se produzcan eventos críticos en los logs.

RO-22: Funcionalidad de búsqueda
El sistema de observabilidad debe contar con un buscador que permita a los usuarios encontrar información de forma rápida y sencilla.

RO-23: Alarmas señales físicas

El sistema debe permitir la configuración de alarmas personalizadas para cada señal proveniente del campo, con el fin de supervisar el estado del sistema. Cada alarma debe ser configurada con un valor umbral y un tiempo de activación, de forma que cuando se sobrepase el valor umbral durante el tiempo establecido, la alarma se active y genere una notificación al personal encargado de la supervisión del sistema.

RO-24: Alarmas por repetición
La plataforma debe permitir la configuración de alarmas basadas en la repetición de eventos, donde se puedan definir el número de veces que debe ocurrir un evento en un período de tiempo determinado antes de que se genere una alarma.

RO-25: Alarmas temporales programadas
La aplicación debe permitir la programación de alarmas temporales basadas en la no variación del valor de una señal durante un período de tiempo T. El usuario debe poder configurar el valor de T y asignar una señal específica para cada alarma temporal. Cuando se cumpla la condición de no variación durante el tiempo T, se debe generar una alarma para alertar al usuario.

RO-26: Temporización de alarmas configurables por tipo
La plataforma debe permitir la temporización de la aparición de las alarmas, de manera que se pueda retrasar su activación hasta un tiempo T configurable según el tipo de alarma. Esto permitirá al usuario configurar el comportamiento del sistema ante situaciones específicas, evitando la generación de alarmas innecesarias y proporcionando información más precisa sobre la situación del sistema.

RO-27: Categorización de alarmas
La plataforma debe permitir la categorización de las alarmas generadas, de manera que se puedan aplicar políticas de tratamiento de alarmas a todas las alarmas de una misma categoría. Esta funcionalidad debe ser configurable por los usuarios con permisos de administración del sistema y debe permitir una gestión eficiente de las alarmas generadas en el sistema.

RO-28: Jerarquización de alarmas
La plataforma debe permitir la jerarquización de las alarmas para organizarlas en una estructura de alarma principal y subordinadas, de manera que las subordinadas se agrupen bajo la principal y se muestren de manera clara y ordenada en la interfaz de usuario. Cada alarma debe tener un nivel de prioridad y las alarmas principales deben tener la capacidad de activar o desactivar todas las alarmas subordinadas relacionadas.

RO-29: Permanencia de las alarmas
La plataforma debe permitir la configuración de diferentes tipos de alarmas, incluyendo alarmas de resolución automática y alarmas que requieren atención manual del operador. Las alarmas de resolución automática deben ser eliminadas automáticamente una vez que la causa que las generó desaparece, mientras que las alarmas que requieren atención manual deben permanecer activas hasta que el operador las resuelva o las cancele manualmente. El sistema debe proporcionar una clara distinción visual y auditiva entre estos dos tipos de alarmas para evitar confusiones y errores en la gestión de las mismas.

RO-30: Sumario de alarmas
La plataforma debe contar con un sumario de alarmas personalizable que permita al usuario visualizar de forma clara y concisa el estado de todas las alarmas generadas por el sistema, incluyendo información relevante como la descripción de la alarma, la hora y fecha en que se

generó, su nivel de prioridad y su estado actual (activa, resuelta, ignorada, etc.). Además, el sumario debe permitir la personalización de las alarmas mostradas en función de diferentes criterios, como la prioridad, la categoría, el tipo de alarma, entre otros, para facilitar la identificación y resolución rápida de las alarmas más críticas.

RO-31: Configuración sumarios de alarmas
La plataforma debe permitir la configuración de múltiples sumarios de alarmas, cada uno con un conjunto específico de alarmas seleccionadas, para que los usuarios puedan visualizar diferentes tipos de alarmas de manera simultánea y personalizada según sus necesidades y áreas de responsabilidad.

RO-32: Silenciado de alarmas
La plataforma debe permitir a los operadores autorizados silenciar temporalmente o suprimir ciertas alarmas de la lista de alarmas activas por un período determinado, con la opción de introducir un motivo para esta acción. Los operadores podrán reactivar las alarmas en cualquier momento y deberán justificar la eliminación temporal de las mismas en el sistema.

RO-33: Visualización y personalización de alarmas
La plataforma debe permitir la configuración de múltiples sumarios de alarmas, cada uno con un conjunto específico de alarmas seleccionadas, para que los usuarios puedan visualizar diferentes tipos de alarmas de manera simultánea y personalizada según sus necesidades y áreas de responsabilidad.

RO-34: Configuración sumarios de alarmas
La plataforma debe permitir la personalización de los estilos de visualización de las alarmas por parte del cliente, de forma que este pueda adaptar la presentación de las alarmas a sus necesidades y preferencias. La herramienta de "estilos" debe permitir la modificación de elementos como el tamaño y color de la fuente, la posición y tamaño de los iconos, la disposición de los campos de información, entre otros aspectos visuales. Además, cualquier cambio en los estilos debe aplicarse automáticamente a todas las alarmas y sumarios activos en tiempo real.

RO-35: Funcionalidad de búsqueda
La plataforma debe contar con un buscador que permita a los usuarios encontrar información de forma rápida y sencilla. El buscador debe ser capaz de realizar búsquedas por diferentes criterios, como el nombre del equipo, el tipo de señal, el nombre del usuario, entre otros.

RO-36: Funcionalidad segmentación de usuarios
La plataforma debe permitir la segmentación de roles y permisos de los usuarios: La aplicación debe ser capaz de asignar diferentes roles y permisos a los usuarios, de manera que cada usuario tenga acceso solo a las funcionalidades y datos que le correspondan. Los roles y permisos deben ser definidos por los administradores del sistema y deben poder ser modificados en cualquier momento.

RO-37: Funcionalidad gestión de usuarios
La gestión de usuarios debe ser fácil y permitir la creación, modificación y eliminación de usuarios de forma sencilla y segura: La aplicación debe permitir a los administradores del sistema la creación, modificación y eliminación de usuarios de forma sencilla y segura. Los usuarios deben ser autenticados antes de poder acceder a la aplicación y deben ser identificados por un nombre de usuario y una contraseña segura.

RO-38: Funcionalidad auditoria de usuarios
La plataforma debe ser capaz de registrar las acciones realizadas por cada usuario, así como la hora y fecha en que se realizaron. Esta información debe ser fácilmente accesible por los administradores del sistema, permitiendo la identificación de posibles problemas o vulnerabilidades.

RO-39: Funcionalidad de segmentación de roles
La plataforma debe permitir la configuración de roles y permisos de forma granular, de manera que los administradores del sistema puedan asignar permisos específicos a cada usuario. Esto permitirá un mayor control y seguridad de los datos y funcionalidades de la aplicación.

RO-40: Funcionalidad seguridad de usuarios
La aplicación debe ser capaz de notificar a los administradores del sistema sobre posibles violaciones de seguridad, como intentos de acceso no autorizados o cambios en la configuración de roles y permisos.

6.1.5 Licencias plataforma IIoT

Se deberá suministrar un sistema de licenciamiento de la plataforma IIoT en formato de suscripción anual, con soporte de de 8x5x12 según ítem 9 del presupuesto *(9. Suministro SW - Licencias - IIoT Digitalization Platform - Subscription anual)*. El software además de los componentes necesarios para monitorizar todo el flujo de datos del ecosistema IIoT (software y hardware) debe permitir la creación de dashboard o cuadros de mando, la interconexión con sistemas auxiliares (GMAO, SAP,...),

Más concretamente los requerimientos son:

RL-01: Precio de licenciamiento
La aplicación debe cumplir con las regulaciones y leyes locales relacionadas con la venta y distribución de software en España, y los precios de las licencias deben ser claramente indicados en euros en una lista de precios pública para garantizar la transparencia y accesibilidad para los clientes potenciales en el mercado español.

RL-02: Adquisición de licencias
La adquisición de licencias para la plataforma sólo puede realizarse mediante una de las tres modalidades siguientes:

1. Licencias perpetuas: Las licencias pueden ser adquiridas por Aigües de Barcelona con un pago único al inicio del proyecto. En esta modalidad de licenciamiento, las extensiones pueden implicar la adquisición de nuevas licencias o ampliación de las existentes, por incremento en el número de señales, incremento en el número de usuarios, incremento de datos históricos, etc.
2. Licencias por suscripción: Las licencias pueden ser adquiridas mediante el pago de una tarifa anual que incluirá el uso de las licencias acordadas y su mantenimiento.
3. Licencias por créditos: El proveedor deberá permitir al cliente la compra de una bolsa de créditos que podrá canjear por cualquiera de las licencias integradas en el portafolio de soluciones. La forma de adquirirlos será la siguiente:

- El usuario adquiere paquetes de créditos anualmente, con pago anual.
- Cada licencia supone un número determinado de créditos.

- El número de créditos puede incrementarse o reducirse a la finalización del contrato.
- No se requiere compromiso de software, y es posible utilizar cualquier software incluido dentro de la modalidad por créditos.
- La actualización de software y soporte están incluidos.

RL-03: Dimensionamiento de las licencias
El sistema de licenciamiento debe ser dimensionado para soportar un número mínimo estimado de:

- NÚMERO DE USUARIOS: 50 UD
- NODOS DE CONEXIÓN (tipo subscriptor): 1 - 5 UD
- NÚMERO DE ACTIVOS MÁXIMO: 10.000 UD

*Dependiendo de la estructura y configuración de la plataforma a nivel de activos, este número puede variar; un activo puede incluir varios nodos y cada nodo disponer de una serie de registros.

La plataforma debe ser capaz de manejar adecuadamente la asignación y el seguimiento de las licencias correspondientes a todos los usuarios, con el fin de garantizar que se cumpla con el requisito de capacidad de usuarios establecido.

6.1.6 Sistema de data streaming

Se deberá suministrar un sistema de suministro de datos (data streaming) y realizar la configuración del este para el suministro de datos a las siguientes fuentes de destino:

a) Gemelo digital
b) Sitec
c) Creapro
d) Plataforma de monitorización de energía
e) Dinapsis Control Data Center
f) SCADA
g) Otros.

El ítem 5 del presupuesto hacer referencia a dicha partida para la creación de los pipeline de datos que interconectará todo el ecosistema de IIoT, desde la ingesta de datos, hasta proveer (poner a disposición) toda esta información en todas las capas superiores, nivel 2.5, 3.0 y 3.5 *(5. Instalación y PeM - Edge - Instalación y configuración de nodos de Data Streaming).*

Requisitos funcionales del sistema de flujo de datos (RS). Funciones y características mínimas que debe cumplir el procesamiento y streaming de datos en la plataforma.

RS-01: Capacidad de distribución
El sistema debe ser capaz de distribuirse en múltiples nodos de forma independiente, lo que permite que cada componente del sistema tenga su propio entorno y recursos aislados. Esto garantiza la escalabilidad y disponibilidad del sistema, ya que permite que el sistema se adapte a las demandas cambiantes del entorno sin afectar el rendimiento del sistema.

RS-02: Capacidad de reenvío tras recuperación

Los nodos deben ser capaces de almacenar temporalmente (mínimo de 7 días) los datos recopilados hasta que se restablezca la conexión con el servidor y se pueda realizar la transferencia de datos. De esta manera, se garantiza la continuidad del monitoreo y la adquisición de datos, evitando interrupciones en la operación.

RS-03: Capacidad de ser dockerizable
El sistema debe tener la capacidad de ser dockerizado.

RS-04: Capacidad de ser desplegado mediante orquestadores
El sistema debe tener la capacidad de ser desplegable mediante orquestadores de contenedores. Esto permitirá que el despliegue y mantenimiento del sistema se automatice, lo que reducirá el tiempo y esfuerzo necesarios para administrar el sistema.

RS-05: Enrutamiento de datos
El sistema debe ser capaz de enrutar los datos entre los diferentes nodos y canales de comunicación de manera confiable y segura.

RS-06: Garantizar la entrega de la información
El enrutamiento debe garantizar la entrega de los datos, incluso si algún nodo falla, para garantizar la disponibilidad del sistema.

RS-07: Procesamiento de datos
El sistema debe ser capaz de procesar más de 1000 mensajes por segundo, lo que implica una capacidad de procesamiento significativa.

RS-08: Canal caliente
El sistema debe ser capaz de manejar diferentes tipos de datos en canal caliente ya que los canales calientes manejan datos de alta prioridad que deben procesarse rápidamente.

RS-09: Canal frio
El sistema debe ser capaz de manejar diferentes tipos de datos en canal frío ya que los canales fríos manejan datos de menor prioridad que se pueden procesar más lentamente.

RS-10: Capacidad de ser escalable
El sistema debe estar diseñado para ser capaz de escalar horizontalmente. Esto significa que el sistema debe poder agregar y quitar nodos de manera dinámica para mantener el equilibrio de carga y garantizar el rendimiento y disponibilidad del sistema.

RS-11: Integración sistema de ingesta
El sistema de ingesta debe contar con una API bien definida que permita a los usuarios ampliar los destinos u orígenes del sistema. La API debe ser fácil de usar y bien documentada para que los usuarios puedan integrarla con sus propias aplicaciones y sistemas de forma rápida y sencilla.

RS-12: Bifurcación de los datos
Los puntos intermedios de comunicación de la arquitectura IoT deben contar con la capacidad de bifurcar la información que fluye a través de ellos. Esta bifurcación debe permitir que la información sea enviada simultáneamente a diferentes destinos, permitiendo así la implementación de diferentes flujos de procesamiento de información según los requerimientos del sistema.

RS-13: Servicio de datos a aplicaciones externas
Los sistemas externos podrán alimentarse de todos los datos de la infraestructura desde los brokers de su nivel correspondiente.

RS-14: Manejo simultáneo de consumidores
Los puntos intermedios de comunicación de la arquitectura IoT deben ser capaces de manejar múltiples consumidores de manera simultánea. Esto significa que los datos enviados desde los nodos de sensores o actuadores deben poder ser recibidos y procesados por varios sistemas de destino al mismo tiempo.

RS-15: Soportar grupos de consumidores
Se requiere que los puntos intermedios de comunicación de la arquitectura IoT sean capaces de soportar grupos de consumidores para distribuir la carga de trabajo. Cada grupo de consumidores debe ser capaz de manejar múltiples conexiones simultáneamente y garantizar la equidad en la distribución de datos.

RS-16: Desarrollo de conectores para el flujo de datos
La aplicación debe ser capaz de comunicarse con sistemas receptores de datos mediante el desarrollo de conectores personalizados. Estos conectores deben ser capaces de enviar los datos de forma encriptada y deben requerir credenciales para conectarse con los sistemas receptores de datos y la aplicación. Los conectores deben ser capaces de adaptarse a diferentes tipos de sistemas y formatos de datos, permitiendo la integración con diferentes fuentes de datos y aplicaciones. Además, los conectores deben ser fácilmente configurables y administrables, permitiendo a los usuarios definir y modificar las conexiones de forma rápida y sencilla.

RS-17: Conectores productores
El sistema debe contar con conectores que permitan la producción de información entre los diferentes puntos intermedios de comunicación de la arquitectura IoT, asegurando la integridad de los datos y su correcto flujo a lo largo de la cadena de procesamiento de información.

RS-18: Conectores consumidores
Se requiere que la arquitectura IoT tenga conectores para consumir información de los diferentes sistemas intermedios de comunicación, permitiendo la integración de datos en tiempo real provenientes de diversas fuentes. Estos conectores deben ser capaces de procesar grandes cantidades de datos y soportar diferentes formatos de datos, asegurando la interoperabilidad con otros sistemas de terceros. Además, deben permitir la configuración de filtros para la selección de datos específicos y la transformación de datos para adaptarse a los requerimientos de la aplicación.

RS-19: Contenido del log
Los logs de la aplicación deben contener información precisa, incluyendo hora de registro, gravedad del evento, origen del evento y una descripción detallada del mismo.

RS-20: Políticas de logs
La gestión de logs debe ser fácilmente configurable, permitiendo a los usuarios definir y modificar las políticas de registro de forma rápida y sencilla.

RS-21: Almacenamiento de logs
Los logs de la aplicación deben ser almacenados de forma segura y protegidos contra pérdidas de datos.

RS-22: Comunicación unidireccional
La aplicación debe asegurar que el flujo de información sea unidireccional, desde los nodos hacia el servidor centralizado, y que cualquier otra comunicación, como el envío de órdenes o configuraciones hacia los nodos, debe ser realizada mediante suscripciones o polling controlados por el servidor centralizado. Se debe garantizar la seguridad de la comunicación entre los nodos y el servidor a través de mecanismos de autenticación y encriptación de extremo a extremo, como mínimo mediante TLS 1.2, para proteger la integridad y confidencialidad de los datos transferidos y evitar posibles vulnerabilidades de seguridad.

RS-23: Comunicación segura
La aplicación debe contar con un registro de actividades y alertas que permita detectar cualquier intento de acceso no autorizado o de intrusiones a la red de comunicaciones. En resumen, la aplicación debe garantizar que la comunicación entre los nodos y el servidor sea segura y confiable, protegiendo los datos y la información que se está transmitiendo.

RS-24: Arquitectura multinivel
La aplicación de ingesta debe implementar una arquitectura de capas/niveles que permita la separación de roles y la independencia entre aplicaciones IT y OT. Para ello, se deberán establecer mecanismos de seguridad y control de acceso en cada capa/nivel, de manera que los datos fluyan entre ellos de forma segura y controlada.

RS-25: Segmentación de permisos por niveles
La aplicación debe contar con un sistema de identificación y autenticación que permita la asignación de permisos y roles a los usuarios en cada nivel, garantizando así la protección de los datos sensibles y la integridad del sistema en su conjunto.

6.1.7 Requisitos de implementación

El hardware necesario para realizar la ingesta de datos se localizará en los emplazamientos:

- EDAR Baix Llobregat
- EDAR Sant Feliu
- EDAR Gavá
- EDAR Besós
- EDAR Montcada

El Edge instalado en estos emplazamientos se encargará de recolectar toda la información de esa estación y de las estaciones dependientes. Cuando se realice la instalación del Industrial PC se realizará una verificación de que todas las variables se están leyendo de forma correcta. Tras la puesta en marcha del sistema se emite un informe que incluye evidencias de que todas las variables obtenidas con el Edge están siendo publicadas en el bróker del sistema superior.

El flujo de información también se ha de tratar como un requisito funcional. El Edge local de cada una de las estaciones debe obtener los datos de todos los equipos de campo utilizando diferentes protocolos industriales que se determinarán en función del origen de los datos. Estos protocolos pueden ser Modbus, OPC UA, MQTT, Ethernet IP de Rockwell o S7. Tras esto realizará una publicación de datos en el Data Streaming localizado en el nivel 2,5.

El data pipeline situado en este nivel será el encargado de publicar en el bróker del nivel 3. El Data Pipeline puede realizar diferentes tareas, como el filtrado de datos, la normalización de datos, la agregación de datos, o cualquier otra tarea necesaria para preparar los datos para su envío al siguiente nivel. A su vez, el pipeline del nivel 3 publicará los datos en el bróker del siguiente nivel.

Los datos se encontrarán accesibles para todas las nuevas aplicaciones en el data path de cada nivel.

Cuando la aplicación se ejecute en la nube los datos serán subidos a esta a través de un pipeline localizado en el nivel 2,5.

Como resultado de la integración de todos los sistemas se puede definir el siguiente flujo de comunicaciones entre los diferentes elementos que forman el sistema:

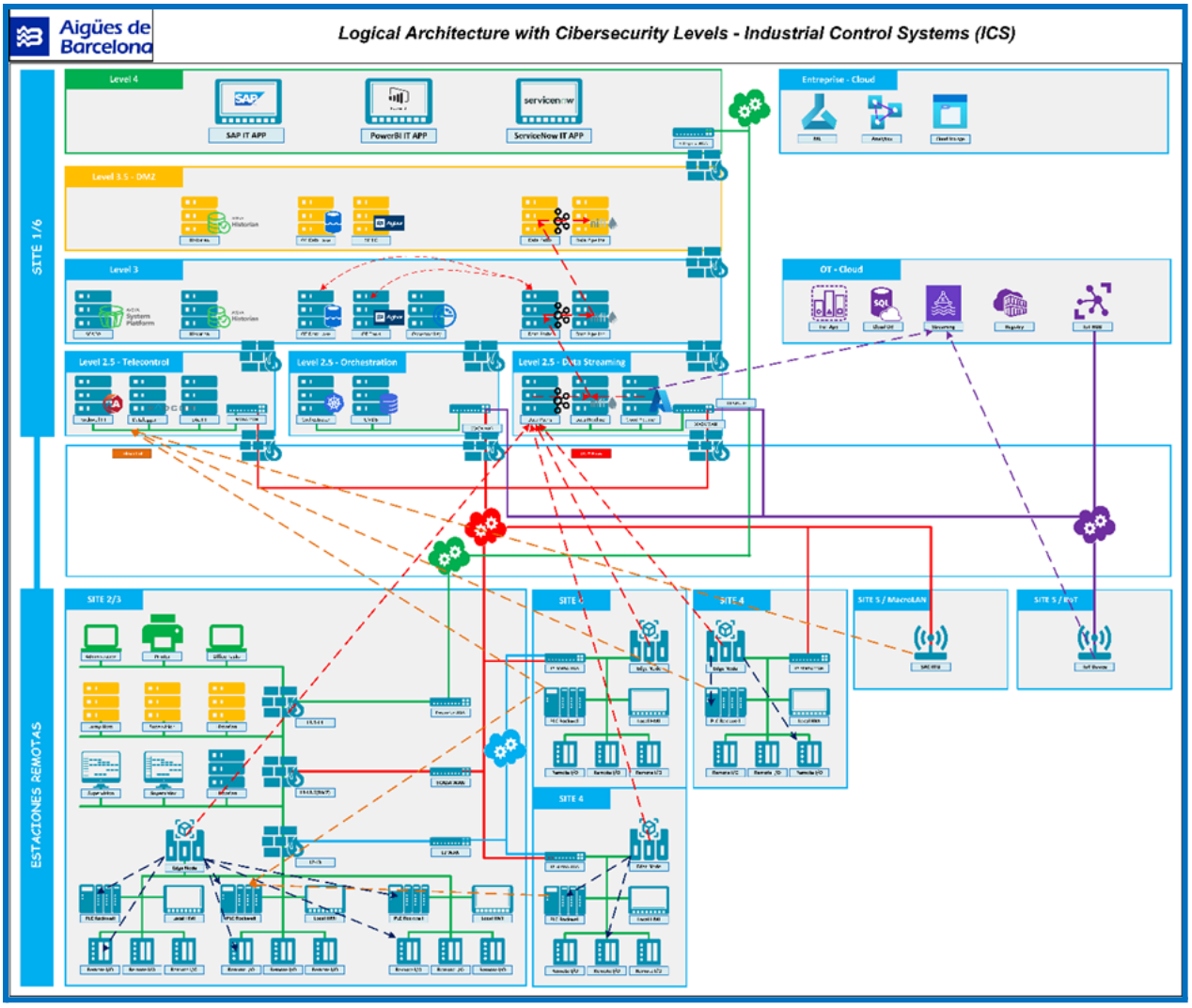


Figura 5. Flujo de comunicaciones plataforma IIoT

Dada esta información se definen los siguientes requisitos funcionales:

RFI-001: Obtención de datos Edge

El Edge local de cada estación debe obtener datos de todos los equipos de campo utilizando diferentes protocolos industriales (Modbus, OPC UA, MQTT, Ethernet IP, S7…) que se determinarán en función del origen de los datos.

RFI-002: Publicación de datos Edge
Después de obtener los datos, el Edge local debe publicarlos en el Data Streaming localizado en el nivel 2,5 utilizando sistemas de transmisión de datos estándar.

RFI-003: Procesamiento de datos
El Data Pipeline situado en el nivel 2,5 debe tener la capacidad de procesar los datos obtenidos, realizar tareas como el filtrado, la normalización, la agregación y cualquier otra tarea necesaria para preparar los datos para su envío al siguiente nivel.

RFI-004: Publicación de datos en el nivel 3
El Data Pipeline del nivel 2,5 debe publicar los datos procesados o sin procesar en el bróker del nivel 3 con sistemas de transmisión de datos estándar.

RFI-005: Acceso a los datos
Los datos deben ser accesibles para todas las nuevas aplicaciones en el Data Path de cada nivel. El acceso de datos se realizará utilizando metodologías estándar.

RFI-006: Subida de datos a la nube
Se debe integrar un pipeline en el nivel 2,5 con la capacidad de enviar y recibir datos de servicios ejecutados en el Cloud. La transmisión de datos se realizará utilizando metodologías estándar.

RFI-007: Sistema de transmisión modular
La metodología de transmisión de datos será estándar para asegurar que todos los servicios que forman parte de la transmisión de datos podrán ser sustituidos por otros sistemas sin interferir en el correcto funcionamiento del resto de servicios.

RFI-008: Capacidad de reenvío tras recuperación
En caso de pérdida de comunicación cada uno de los módulos que forman la infraestructura debe ser capaz de almacenar temporalmente (mínimo 7 días) los datos recopilados en cada uno de sus nodos, y realizar un reenvío de estos datos cuando se restablezca la comunicación con el siguiente elemento de la cadena de subida de datos.

Los equipos Edge están diseñados para procesar datos y realizar análisis en tiempo real cerca de la fuente de los datos. Esto tiene la ventaja de reducir la latencia en la transmisión de datos a través de la red, mejorar la seguridad y disminuir la carga en los servidores centrales.

Para realizar la tarea de ingesta, se configurarán las aplicaciones desplegadas en el equipo Edge para que se conecte a cada uno de los orígenes de datos necesarios y obtenga todas las variables definidas en el archivo mapping "Datos a enviar a sistema IIoT" (Archivo incluido en anexo 4). Esto puede requerir la ejecución por parte del proveedor de nuevas conexiones y la configuración de protocolos específicos para cada origen de datos.

Una vez que se han obtenido los datos de cada origen de datos, se configurará la subida de datos al Data Streaming del nivel 2,5. La subida de datos implica enviar los datos recopilados a un sistema centralizado donde se pueden almacenar, procesar y analizar para obtener información útil.

Las aplicaciones desplegadas tienen la capacidad de ampliar tanto el número de fuentes de datos como el número de variables que se obtienen de cada una de estas fuentes.

6.2 Lote 2: Requerimientos técnicos ámbito TI y ciberseguridad

Este apartado describe las necesidades de compra en hardware y licencias para cubrir los requerimientos técnicos para la integración de la plataforma IIoT.

Los equipamientos o servicios a desplegar en el Centro de Proceso de Datos (CPD) de Aigües de Barcelona, o en cualquier armario de comunicaciones de los centros, seguirán las políticas corporativas de despliegue de Aigües de Barcelona y deberán ser analizadas y integradas en la ejecución de tareas por parte del adjudicatario.

Cualquier otro equipamiento, hardware y/o software necesario para la correcta ejecución y despliegue del sistema de información ofertado, así como su óptimo funcionamiento, deberá ser suministrado por el adjudicatario.

El plazo de entrega de todos los productos adquiridos será de un máximo de 4 semanas desde la entrada en vigor del contrato. El hardware adquirido debe ser nuevo, el adjudicatario debe poder aportar un documento de fabricante que certifique que es así.

6.2.1 Implementación de servidores ESXi CPD

Para poder garantizar el correcto funcionamiento de la plataforma, se aprovisionarán dos servidores ESXi que irán destinados al CPD de Aigües de Barcelona. Con estos dos servidores se espera asegurar la alta disponibilidad y dar la capacidad necesaria para un correcto funcionamiento de las máquinas virtuales que serán aprovisionadas en dichos servidores.

También se espera cubrir un posible futuro crecimiento (escalabilidad de la plataforma).

Para ello se solicita que cumplan unas características mínimas para la correcta adaptación de los servidores al CPD:

- Doble fuente de alimentación,
- Formato enrackable en armarios de 19”
- Contendrá todos los elementos para su correcta instalación (guías, hardware de instalación, tornillería, latiguillos, cableado, fibras, etc.)

6.2.2 Ampliación servidores EDAR

Con el fin de poder dar redundancia a los servidores de las EDAR's para el correcto funcionamiento de la plataforma IIoT, se dispondrá a añadir una ampliación de los servidores actuales en las mismas, lo que garantizará la alta disponibilidad de los servidores. Esta redundancia de los servidores solamente será necesario en las EDARS de Sant Feliú de Llobregat, Montcada i Reixac y Gava-Viladecans, ya que las EDAR's de Baix Llobregat i Besós ya disponen de esta.

Debido a que el hardware de la EDAR de Montcada es diferente al de las EDAR's de Sant Feliú de Llobregat y Gavá-Viladecans, la ampliación tendrá unas necesidades diferentes a éstas.

6.2.3 Requisitos Hardware CPD

Componentes	Cantidad
Modelo: HPE ProLiant DL380 Gen10 Plus 8SFF NC Configure-to-order incluye: ○ 32-DIMM slots ○ Storage Controller embedded with 14 SATA ports. ○ PCIe: Three standard in primary riser ○ Drive Cage: 8 SFF - SAS/SATA ○ 4 Standard Fans ○ HPE iLO with Intelligent Provisioning (standard) ○ 2U Rack form factor	x2
Intel Xeon-Gold 6334 3.6GHz 8-core 165W Processor for HPE o superior	x4
HPE 64GB (1x64GB) Dual Rank x4 DDR4-3200	x32
HPE DL38X Gen10 Plus x8/x16/x8 Secondary Riser Kit	x2
Broadcom BCM57416 Ethernet 10Gb 2-port BASE-T Adapter for HPE	x4
Tarjeta de 2 puertos de fibra SFP+ 10 Gbps para conexión a LAN (transceivers incluidos)	x2
Transceivers de fibra SFP+ 10 Gbps installables a switches Cisco Nexus model N3K-C3172PQ-X	x4
Tarjeta de fibra (one port) para conexión a SAN 16 Gbps	x4

Broadcom 1Gb 4-port BASE-T	x2
HPE 800W Flex Slot Platinum Hot Plug Low Halogen Power Supply Kit	x4
HPE iLO Advanced 1-server License with 3yr Support on iLO Licensed Features	x2
Guías para instalación en armario RACK	x2
Cable FC OM4 3m	x4
Cable UTP Rj45 3m Cat6	x10
Cable UTP Rj45 3m Cat6a	x8
Cables de fibra para conectividad SFP +10Gbps LAN 3M	x4

6.2.4 Mantenimiento hardware y licencias para el CPD

Componentes	Cantidad
Licencias Windows Datacenter 2022 + Software assurance (16 cores) 3yr	x2
VMware vSphere Enterprise Plus 1 Processor 3yr E-LTU	x4
VMware vRealize Operations Advanced per CPU 3yr E-LTU	x4

6.2.6 Servicios profesionales CPD

Fase 0. Gestión del proyecto

- Apertura, seguimiento y cierre del proyecto.

Fase 1. Análisis del diseño.

- Análisis de la infraestructura, validación del diseño.

Fase 2. Startup plataforma física

Startup servidores HPE DL380 Gen10

- Desembalado e inventariado de componentes.

- Ensamblado y enrackado de 1 servidor HP Proliant DL380 Gen10.
- Conexionado a la alimentación, arranque y revisión del hardware.
- Configuración de las interfaces de gestión (iLO).
- Verificación y actualización del firmware.
- Inicialización de disco y configuración de RAID.
- Conectividad LAN a la red del cliente y etiquetado.

Configuración entorno VMware

- Instalación de VMware ESXi en 1 servidores (1 x DL380 Gen10).
- Instalación y actualización VMware vCenter.
- Configuración de parámetros de red según requisitos de cliente.
- Comprobación y/o reconfiguración del diseño característica y conexión a vCenter (HA, vMotion, etc.)
- Alta del nuevo servidor ESX en el clúster VMware.
- Presentación datastores a nuevos hosts.
- Verificación del correcto funcionamiento del entorno.

Fase 3. Documentación

- Documentación de proyecto.
- Aceptación del proyecto y cierre.

6.2.7 Requisitos Hardware Sant Feliú de Llobregat y Gava-Viladecans

Componentes	Cantidad
Modelo: HPE ProLiant DL360 Gen10 8SFF incluye: ○ 24-DIMM slots (12 can be used for NVDIMMs or 12 can be used for HPE ○ Persistent Memory) ○ Embedded SW RAID (S100i) with 14 SATA ports ○ 2 PCIe slots (1 x16 FH / 1 x8 LP) ○ Drive Cage: 8 SFF - SAS/SATA ○ 1 CPU – 5 Standard Fans - 2 CPU – 7 Standard Fans ○ HPE iLO with Intelligent Provisioning (standard) ○ 1U Rack form factor	x2
HPE 64GB (1x64GB) Dual Rank x4 DDR4-2933	x16
HPE 480GB SATA 6G Mixed Use SFF BC Multi Vendor SSD	x4
Intel Xeon-Silver 4214 (2.2GHz/12-core/85W) FIO Processor Kit	x2

HPE Ethernet 1Gb 4-port FLR-T I350-T4V2 Adapter	x2
HPE 800W Flex Slot Platinum Hot Plug Low Halogen Power Supply Kit	x4
HPE 600GB SAS 12G Mission Critical 15K SFF BC 3-year Warranty HDD	x8
Ethernet 10Gb 2-port BASE-T	x6
HPE 96W Smart Storage Lithium-ion Battery with 145mm Cable Kit	x2
HPE iLO Advanced 1-server License with 3yr Support on iLO Licensed Features	x2
HPE ProLiant DL36x Gen10 Plus 8SFF SAS/SATA PCIe Slot2 Tri-Mode Cable Kit	x2
HPE 1U Gen10 SFF Easy Install Rail Kit	x2
Cable de red RJ45 UTP CAT6 3m	x15
Cable Cat6a 3m RJ45	x12

6.2.9 Mantenimiento hardware y licencias para Sant Feliú de Llobregat y Gava-Viladecans

Componentes	Cantidad
Licencias Windows Datacenter 2022 + Software assurance (16 cores) 3 yr	x2
HPE 3Y Tech Care Service 24x7	x1
HPE DL360 Gen10 Support	x2

6.2.10 Ampliación Sant Feliu y Gavá para Hiperconvergencia

Componentes	Cantidad
Intel Xeon-Silver 4214 (2.2GHz/12-core/85W) for HPE ProLiant DL360 Gen10	x2
HPE 600GB SAS 12G Mission Critical 15K SFF SC 3-year Warranty Multi Vendor	x2
HPE Ethernet 10Gb 2-port BASE-T BCM57416 Adapter	x4

Componentes	Cantidad
Cable Cat6a 3m RJ45	x12

6.2.11 Requisitos Hardware Montcada i Reixac

Componentes	Cantidad
Modelo: HPE ProLiant DL360 Gen10 8SFF incluye: ○ 24-DIMM slots (12 can be used for NVDIMMs or 12 can be used for HPE ○ Persistent Memory) ○ Embedded SW RAID (S100i) with 14 SATA ports ○ 2 PCIe slots (1 x16 FH / 1 x8 LP) ○ Drive Cage: 8 SFF - SAS/SATA ○ 1 CPU – 5 Standard Fans - 2 CPU – 7 Standard Fans ○ HPE iLO with Intelligent Provisioning (standard) ○ 1U Rack form factor	x1
HPE 64GB (1x64GB) Dual Rank x4 DDR4-2933	x12
HPE 480GB SATA 6G Mixed Use SFF BC Multi Vendor SSD	x2
Intel Xeon-Silver 4214 (2.2GHz/12-core/85W) FIO Processor Kit	x1
HPE Ethernet 1Gb 4-port FLR-T I350-T4V2 Adapter	x1
HPE 800W Flex Slot Platinum Hot Plug Low Halogen Power Supply Kit	x2
HPE 600GB SAS 12G Mission Critical 15K SFF BC 3-year Warranty HDD	x4
2 HPE 2TB SAS 12G Business Critical 7.2K SFF SC 1-year Warranty 512e HDD	x2
Ethernet 10Gb 2-port BASE-T	x2
HPE 96W Smart Storage Lithium-ion Battery with 145mm Cable Kit	x1
HPE iLO Advanced 1-server License with 3yr Support on iLO Licensed Features	x1
HPE ProLiant DL36x Gen10 Plus 8SFF SAS/SATA PCIe Slot2 Tri-Mode Cable Kit	x1
HPE 1U Gen10 SFF Easy Install Rail Kit	x1

Componentes	Cantidad
Cable de red RJ45 UTP CAT6 3m	x4
Cable Cat6a 3m RJ45	x4

6.2.13 Mantenimiento hardware y licencias Montcada i Reixac

Componentes	Cantidad
Licencias Windows Datacenter 2022 + Software assurance (16 cores)	x1
HPE 3Y Tech Care Service 24x7	x1
HPE DL360 Gen10 Support	x1

6.2.14 Ampliación Montcada i Reixac para Hiperconvergencia

Componentes	Cantidad
Intel Xeon-Silver 4214 (2.2GHz/12-core/85W) for HPE ProLiant DL360 Gen10	x1
HPE 600GB SAS 12G Mission Critical 15K SFF SC 3-year Warranty Multi Vendor	x1
HPE Ethernet 10Gb 2-port BASE-T BCM57416 Adapter	x2
Cable Cat6a 3m RJ45	x4

6.2.15 Servicios Profesionales EDARS (SF, Gavá, Montcada)

Fase 0. Gestión del proyecto

- Apertura, seguimiento y cierre del proyecto.

Fase 1. Análisis del diseño

- Análisis de la Infraestructura, validación del diseño.

Fase 2. Startup plataforma física

Startup 3 servidores HPE DL360 Gen10, uno por site

- Desembalado e inventariado de componentes.
- Ensamblado y enrackado de 1 servidor HP Proliant DL360 Gen10.
- Conexionado a la alimentación, arranque y revisión del hardware.
- Configuración de las interfaces de gestión (iLO).
- Verificación y actualización del firmware.
- Inicialización de disco y configuración de RAID.
- Conectividad LAN a la red del cliente y etiquetado.

Startup 3 servidores actuales HPE DL360 Gen10 con las ampliaciones adquiridas

- Desembalado e inventariado de componentes.
- Ensamblado y enrackado de 1 servidor HP Proliant DL360 Gen10.
- Conexionado a la alimentación, arranque y revisión del hardware.
- Configuración de las interfaces de gestión (iLO).
- Verificación y actualización del firmware.
- Inicialización de disco y configuración de RAID.
- Conectividad LAN a la red del cliente y etiquetado.

Configuración entorno Hyper-V

- Instalación de Sistema Operativo WS2019 e Hyper-V en los 3 servidores DL360.
- Instalación, características y roles para todos los nodos.
- Configuración de red.
- Configuración Almacenamiento compartido
- Configuración del entorno de Hyper-V / creación de Failover Cluster. 2 por centro.
- Validar la configuración del clúster.
- Creación de hasta 6 MV por centro
- Comprobación de la integridad del entorno virtual.
- Verificación del correcto funcionamiento del entorno.

Configuración entorno Hyper-V en servidor temporal de paso para no parar servicio

- Instalación, características y roles para servidor temporal. El servidor se usará en modo secuencial por centro.
- Instalación de Sistema Operativo WS2019 e Hyper-V.
- Instalación, características y roles para aceptar servicio del nodo actual.
- Configuración de red.
- Configuración del entorno de Hyper-V.
- Validar la configuración del clúster.
- Creación de hasta 6 MV por centro.
- Comprobación de la integridad del entorno virtual.
- Verificación del correcto funcionamiento del entorno.

Fase 3. Documentación

- Documentación de proyecto.
- Aceptación del proyecto y cierre.

6.2.16 Requerimientos técnicos ciberseguridad

Las diversas estaciones depuradoras de aguas residuales (EDARs) de AB albergan sistemas de información que dan soporte al proceso industrial de la depuración y los sistemas de saneamiento en alta metropolitanos. Estos sistemas son considerados OT (Operational Technologies). Estos sistemas soportan la automatización y el control de los procesos, así como sistemas de información operativos y por lo tanto son esenciales para el correcto funcionamiento de los sistemas de saneamiento en alta metropolitanos.

Actualmente la compañía se enfrenta a nuevas amenazas en materia de cibercriminalidad. Los sistemas informáticos en general son la base de la mayoría de los procesos de la compañía y defender y protegerlos de las amenazas es la prioridad de la Dirección de Seguridad. En concreto, los sistemas OT, de las EDAR's y otros sistemas de saneamiento en alta, suponen un punto clave y deben estar suficientemente protegidos.

Tras un análisis de riesgos, se evidenció la urgente necesidad de establecer nuevos sistemas de control y defensa de la infraestructura OT. Con anterioridad, AB abordó este tipo de proyectos en otras infraestructuras de AB. Se pretende ampliar estas soluciones ampliando el ámbito protegido extendiendo las soluciones al resto del entorno OT.

Es básico ampliar las infraestructuras ya existentes para lograr eficiencias de inversión y de gestión. Por ello, se detallan los elementos necesarios para cada una de ellas, lograr una mitigación de riesgos cibernéticos suficiente y dotar de una protección adecuada a cada planta.

6.2.17 Ciberseguridad equipos OT

Los sistemas de saneamiento en alta, gestionados por Aigües de Barcelona, albergan sistemas de información que dan soporte a la operación de los procesos. Estos sistemas son considerados OT (Operational Technologies). Estos sistemas soportan la automatización, control y supervisión de los procesos, y por lo tanto, son esenciales para el correcto funcionamiento de los sistemas.

Actualmente, Aigües de Barcelona se enfrenta a nuevas amenazas en materia de cibercriminalidad. Los sistemas informáticos en general son la base de la mayoría de los procesos de la compañía y defender y protegerlos de las amenazas, es la prioridad de la Dirección de Seguridad. En concreto, los sistemas OT de los sistemas de saneamiento en alta son infraestructuras clave, desde el punto de vista sanitario y medioambiental del territorio, y deben estar suficientemente protegidas.

Las soluciones tipo a implementar serán básicamente de fortificación y bastionado de los servidores.

6.2.17.1 Fortificación servidores y clientes de operación

Aigües de Barcelona ya tiene desplegada en estos momentos la solución “Endpoint Threat Protection” de McAfee para la protección de los equipos y sistemas de información y control del ámbito OT de otros sistemas operativos, por lo cual se instalará esta misma solución en los nuevos requerimientos que surgen del desarrollo de la infraestructura necesaria para la implementación de la plataforma IIoT, ya que añadir antivirus de la misma marca supone una innumerable gama de ventajas al respecto de la integración y de la gestión de la ciberseguridad en estas instalaciones.

Adicionalmente al Sw de antivirus se requerirán dos elementos más de la suit de productos McAfee: el controlador de dispositivos y el controlador de aplicaciones.

Todos los productos de la Suit McAfee ya implementados en Aigües de Barcelona están integrados en la consola de gestión de McAfee disponible de Aigües de Barcelona, centralizándose allí todos los eventos y registros (logs) consiguiendo un repositorio único.

Por todo lo anterior, no se requiere por parte del proveedor presupuestar el proyecto de instalación y despliegue.

Política de bastionado de equipos

Se requiere desplegar esta solución en los nuevos sistemas a desarrollar en la implementación de la plataforma IIoT en los sistemas de saneamiento. El uso de los diferentes productos de la Suit dependerá de la función del equipo a defender:

- **Servidores:** Los servidores son la parte más crítica de los sistemas de información y control de los sistemas operativos, por eso debemos prestarle una atención extraordinaria.

    - **McAfee EndPoint Security Threat Prevention (ENS)**
    - **McAfee Device Control (DEC)**

Si el servidor es virtual no será necesario DEC.

- **Clientes de operación y/o supervisión OT:** Se trata de entornos con SO de PC que, al tener una interacción directa con el usuario, no permiten un nivel de bastionado de sistema operativo tan elevado como el caso de los servidores. El uso habitual y continuado del equipo por parte del usuario lo hace más propenso a recibir ataques o a la ejecución de posibles programas maliciosos (conocidos o no), por este motivo se despliega la solución de control de aplicaciones y de dispositivos en los clientes de operación.

- **McAfee Application Control (ACD)**
- **McAfee Device Control (DEC)** (no es necesario si el equipo cliente es virtual)

Detalle de licencias a suministrar (3 años de licenciamiento)

- **30 ut licencias: Endpoint Threat Protection (Perpetual):** Suit de productos entre los que se incluyen:
    - **McAfee EndPoint Security Threat Prevention (ENS):** Solución de antivirus de McAfee orientada a servidores industriales.
    - **McAfee Device Control (DEC):** Permite controlar los dispositivos extraíbles que se conectan a un equipo y bloquear los que no estén permitidos.
- **30 ut licencias: McAfee Application Control (ACD) (Perpetual):** Módulo para el congelado de equipos a través de listas blancas de aplicaciones.

Servicios de implantación y despliegue

No se requieren.

Soporte y mantenimiento

La solución propuesta debe contar con soporte por parte del fabricante, así como acceso a las nuevas versiones. Gold Software Support.

6.2.17.2 Detección de malware avanzado y respuesta a incidentes

Las amenazas de seguridad actuales son cada vez más sofisticadas; en la forma en que seleccionan, atacan e infiltran a las organizaciones para robar sus activos principales.

Es necesaria la implementación de una solución para investigar y generar una respuesta ante un incidente que minimice el impacto potencial de ataques cibernéticos cada vez más sofisticados y dirigidos.

Actualmente, los sistemas OT de otras instalaciones de Aigües de Barcelona ya están usando FireEye, tanto en equipos de cliente como servidores.

Por ello, es básico centralizar este control en una única solución. De esta manera, el repositorio de registros (logs) y evidencias es único y está integrado. De otra manera sería imposible agregar toda esta información y se deberían desarrollar soluciones de integración a medida desbordando el importe de la inversión muy significativamente.

El despliegue de esta misma solución en la nueva infraestructura de sistemas de información operativos supondrá solamente adquirir licencias adicionales, ya que Aigües de Barcelona dispone de la infraestructura necesaria para gestionarlas.

Del mismo modo, no se requiere cotizar el proyecto de instalación y despliegue, pues añadir las nuevas licencias es sumamente sencillo y rápido. Se ampliará el número de licencias aprovechando la infraestructura base ya desplegada.

Política de bastionado de equipos

Todos los equipos tanto servidor como clientes de operación y/o supervisión OT deberán tener instalado FireEye, sin distinción de si se tratan de sistemas físicos o virtuales.

Detalle de licencias (3 años de licenciamiento)

30 ut FireEye Endpoint Security

Servicios de implantación y despliegue

No se requieren.

Soporte y mantenimiento

La solución propuesta debe contar con soporte por parte del fabricante durante el primer año, así como acceso a las nuevas versiones.

6.2.18 Ciberseguridad de equipos IT

La protección de los equipos informáticos tiene una de sus mejores soluciones en el antivirus. Aigües de Barcelona ya tiene desplegada en estos momentos la solución “Deep Security de TrendMicro” para proteger los equipos servidores del ámbito IT. En cuanto a los equipos de trabajo tienen instalado la solución CROWDSTRIKE.

Por todo lo anterior, no se requiere cotizar el proyecto de instalación y despliegue pues añadir las nuevas licencias es sumamente sencillo y rápido.

La estrategia a seguir para el bastionado de los equipos será la descrita a continuación.

6.2.18.1 Fortificación servidores y clientes de operación

La solución de antivirus para los equipos es TrendMicro, se dispone de sendas consolas de gestión (para servidores y equipos de trabajo). Desde estas consolas se gestiona el estado de salud de los equipos y se distribuyen las actualizaciones de firmas, estas deberán ser diarias en la medida de lo posible.

Política de bastionado de equipos

- **En servidores**

  Todos los servidores tendrán instalado Deep Security de TrendMicro. Este agente será instalado por la dirección de sistemas de información y después desde ciberseguridad se desplegarán las configuraciones.

  El agente permanecerá en funcionamiento en todo momento. Estará protegido el proceso de desactivación. Se mantendrá en contacto con la consola para tener gestión sobre él.

  Detalle de licencias (3 años de licenciamiento)

  5 licencias: Deep Security - Malware Prevention y Network Security - per Server (VM)

Soporte y mantenimiento

Las licencias suministradas deberán contar con soporte por parte del fabricante durante el primer año, así como acceso a las nuevas versiones.

6.3 Lote 3: Gestor del Proyecto (PMO)

El principal objetivo del Gestor del Proyecto será la gestión del proyecto para el cumplimiento de la planificación y cronograma del mismo, conseguir los estándares de calidad definidos y el control de los costes dentro de los parámetros económicos definidos en el contrato de cada uno de los proveedores; colaborando con los servicios técnicos de Aigües de Barcelona en la corrección de las posibles desviaciones en cada una de las dimensiones.

Este servicio se asegurará de la correcta ejecución de cada lote; de la coordinación entre los contratistas de los mismos; así como del seguimiento de los procesos y procedimientos asociados a su desarrollo y al de los diferentes sistemas/proyectos relacionados, siguiendo el ciclo de vida completo de las iniciativas que estén relacionadas, en coordinación con los responsables de Aigües de Barcelona, considerando las afecciones de otros proyectos que se lleven a cabo, y en particular de las diferentes actuaciones e iniciativas que se desarrollarán en el marco del proyecto RESSONA de Aigües de Barcelona en el ámbito del saneamiento. Cabe destacar que otras iniciativas estén ejecutándose al mismo tiempo, necesitando una gestión y coordinación eficaz para limitar los impactos cruzados entre los diferentes proyectos.

6.3.1 Obligaciones del PMO

Entre las principales actividades y tareas que forman parte del alcance de este servicio son:

- Coordinación con el equipo de Sistemas de Control Industrial de Aigües de Barcelona en materia de estandarización y criterios del despliegue de la plataforma.
- Proporcionar soporte de gestión de proyectos a los Jefes del Proyecto de Aigües de Barcelona, incluyendo la revisión y asesoramiento en la definición de los objetivos y en la planificación y ejecución de las iniciativas.
- Proporcionar apoyo funcional y técnico al equipo de desarrollo del proyecto, aportando ideas y soluciones a las necesidades planteadas.
- Proporcionar un marco de referencia para el seguimiento y el control de proyectos, para asegurarse que los proyectos se están ejecutando según lo planeado y se están cumpliendo los objetivos del mismo.

    - Planificar el proyecto en todos sus aspectos, identificando las actividades a realizar, los plazos previstos y los recursos necesarios, especificando su dedicación.
    - Velar por la correcta ejecución del proyecto, así como dirigir la coordinación de los diferentes equipos ejecutores.
    - Monitorear el desempeño del proyecto y proporcionar informes de seguimiento a los Jefes de Proyecto y a la dirección de Aigües de Barcelona, asegurando el cumplimiento de los objetivos del proyecto, en cuanto a plazos establecidos, coste y calidad.
    - Participar en las reuniones de inicio, de seguimiento y cierre del proyecto con los proveedores, así como en las que se requieran en el seguimiento post-productivo (periodo de garantía del proyecto).
    - Tomar las acciones necesarias para conocer en todo momento la situación en relación con los objetivos establecidos del proyecto, plazos establecidos y entregas asociadas al proyecto.
    - Adoptar las medidas correctoras pertinentes para poner remedio a las posibles desviaciones que se hubieran detectado.
    - Anticipar posibles riesgos para la consecución de los objetivos del proyecto e iniciar las medidas necesarias para su control y mitigación.
    - Proponer, en su caso, modificaciones a los límites u objetivos básicos del proyecto cuando concurran circunstancias que así lo aconsejen.

- Colaborar en la elaboración de la documentación formal de seguimiento del proyecto ante las administraciones públicas.
- Mantenimiento permanente de las relaciones externas del proyecto: clientes, proveedores, terceros, IT de Aigües de Barcelona, etc. De forma específica, con respecto a los equipos ejecutores del proyecto, mantener la requerida interlocución con los Jefes de Proyecto de Aigües de Barcelona.
- Tramitar y gestionar el ticketing interno para coordinar la realización de las diferentes tareas de los equipos internos, siguiendo los procedimientos establecidos y las herramientas corporativas.

- Asegurar que todo proyecto y entregable cumpla con todos los requerimientos de seguridad y de protección de datos necesarios, validándolo conjuntamente con DPO y el departamento de seguridad de Aigües De Barcelona.
- Valorar diferentes productos u opciones de desarrollo, para escoger la que más se ajuste a las necesidades de Aigües de Barcelona, tanto a nivel de estrategia como a nivel de presupuesto económico del proyecto.
- Validación de definiciones visuales de los sistemas (maquetas y/o mockups) con el fin de asegurar que cumplen con las necesidades del usuario final, obteniendo la validación de estos en caso de ser necesario.
- Revisar los planes de prueba para asegurar que cumplan las especificaciones requeridas por Aigües de Barcelona.
- Ser capaz de llevar a cabo las tareas descritas con anterioridad tanto con metodologías tradicionales como con metodologías de trabajo dinámicas e innovadoras tipo Agile, o incluso con un modelo mixto.

7 CONDICIONES OPERATIVAS DE EJECUCIÓN

7.1 Lote 1: Condiciones operativas en el ámbito de SCI-OT

7.1.1 Cobertura del servicio

El proveedor deberá indicar en su oferta técnica el hardware propuesto para los equipos Edge, equivalente al descrito en el punto 6.1.1.

El proveedor deberá indicar en su oferta la plataforma IIoT propuesta y justificar el cumplimiento de los requisitos descritos en el punto 6.1 y subsiguientes sobre el sistema de orquestación (RFO), sistema de ingesta (RSI), plataforma de observabilidad (RO), licenciamiento (RL), sistema de data streaming (RS) y requisitos funcionales de implementación (RFI).

El servicio de proveedor cubrirá el suministro, instalación, programación y puesta en marcha del hardware y software descritos en el punto 8.1 y subsiguientes, en las ubicaciones definidas.

El proveedor deberá configurar las aplicaciones desplegadas en los equipos Edge para que se conecten a cada uno de los orígenes de datos necesarios y obtenga todas las variables definidas en el archivo mapping "Datos a enviar a sistema IIoT" (anexo 4). Esto puede requerir la creación de nuevas conexiones y la configuración de protocolos específicos para cada origen de datos, como se indica en el punto 6.1.7.

El proveedor deberá configurar la monitorización de la información, los cuadros de mando y las alarmas, según el análisis previo a realizar conjuntamente con los responsables técnicos de AB.

7.1.2 Metodología de trabajo

Se mantendrán reuniones periódicas (mínimo semanales) con los interlocutores de SCI y de gestión de proyecto para informar de los avances de los trabajos.

El proveedor actualizará semanalmente el estado de ejecución de los trabajos respecto a la planificación prevista.

Al inicio de la ejecución, los interlocutores de SCI y de gestión del proyecto abrirán una lista de desviaciones del proyecto que se tratarán semanalmente y el proveedor propondrá soluciones y plazos de resolución.

7.1.3 Equipo de trabajo

El equipo de proyecto debe constar al menos del siguiente personal, si bien dependiendo de la fase del mismo no todo el personal debe estar dedicado a él a tiempo completo. No obstante, todo el equipo debe estar disponible para corregir las desviaciones que puedan surgir en la ejecución del proyecto.

Perfil: Director de proyecto
- Formación: Titulado en ingeniería o ciencias
- Cualificación: Responsable de la gestión y la coordinación del área de desarrollos de la empresa con capacidades de asignación/desasignación de recursos dentro de su propia empresa, así como de la resolución de problemas graves que afecten al desarrollo del proyecto. Certificado de Prince2
- Experiencia: Requeridos al menos 5 años de experiencia como Director de Proyecto o Jefe de Proyectos de servicios

Perfil: Jefe de proyecto
- Formación: Titulado en ingeniería o ciencias
- Cualificación: Capacidad demostrable para la planificación y gestión de proyectos
- Experiencia: Requeridos al menos 4 años de experiencia como Jefe de Proyecto en proyectos

Perfil: Consultor ciberseguridad
- Formación: Titulado en ingeniería o ciencias. Formación específica en ciberseguridad
- Cualificación: Certificación IEC 62443
- Experiencia: Requeridos al menos 4 años de experiencia como consultor de ciberseguridad en proyectos OT.

Perfil: Industrial specialist
- Formación:Titulado en ingeniería o ciencias
- Cualificación: Experiencia demostrable en la ejecución de proyectos similares. Experto en digitalización de entornos industriales e ingesta de datos
- Experiencia: Requeridos al menos 4 años de experiencia como especialista en proyectos de digitalización industrial

Perfil: Coordinador de proyecto / Team manager
- Formación:Titulado en ingeniería o ciencias
- Cualificación:Capacidad demostrable para la planificación y gestión de equipos
- Experiencia: Requeridos al menos 4 años de experiencia como Jefe de Proyecto en proyectos

Perfil: Ingeniero de redes
- Formación: Titulado en ingeniería o ciencias
- Cualificación: Experiencia demostrable en el diseño y despliegue de redes OT, recomendable SIEMENS CEIN – Certified Expert for Industrial Networks o SIEMENS CPIN – Certified Professional for Industrial Network o similares.
- Experiencia: Requeridos al menos 4 años de experiencia en diseño y despliegue de redes OT

Perfil: Técnico en automatización
- Formación: Grado superior en automatización industrial
- Cualificación: Experiencia demostrable en el diseño, configuración y despliegue de arquitecturas de automatización que incluyan PLC-SCADA-Sistemas de Información.

- Experiencia: Requeridos al menos 4 años de experiencia como técnico en automatización en plataformas de Rockwell Automation (ControlLogix), Citect Plant y Siemens PCS7 o similares.

7.1.4 Entregables

- Documentación eléctrica (EPLAN) de los armarios con el hardware instalado.
- Lista de materiales instalados (Excel) con referencias del fabricante y cantidad instalada.
- Modificación de los esquemas eléctricos actuales o generación de nuevos esquemas eléctricos.
- Esquema detallado del armario indicando todos los elementos instalados.
- Tabla especificando el parcheo de conexiones UTP y eléctricas en cada instalación, siendo necesario que entre otros aparezca información como la siguiente: número de toma de red de parcheo, nombre del panel de parcheo, switch al que se conecta, número de puerto del switch, etiqueta del cableado, nombre de equipo/usuario conectado.
- Fotos finales de la instalación, de los alrededores de los racks de securización, su interior y exterior, así como de los firewalls OT y sus alrededores.
- Documentación del fabricante de los equipos instalados: manuales de instalación y mantenimiento, certificados de garantía, licencias, servicio de representación y asistencia técnica.
- Manual detallado sobre la plataforma IIoT implementada y pruebas de validación.
- Manual de operación de la plataforma IIoT, monitorización y supervisión, alarmas, cuadros de mando, etc.
- Documento con la descripción de la red, configuraciones, usuarios y claves.
- Ficheros de configuración de todos los equipos.
- Licencias del software instalado descrito en el punto 8.1 y subsiguientes.
- Cualquier otra documentación que complemente la relación anteriormente expuesta y que se considere necesaria para la explotación (operación y mantenimiento) posterior de la solución desarrollada.

7.1.5 Formación

El proveedor del lote 2 deberá realizar dos formaciones, una dirigida al personal de mantenimiento de la plataforma IIoT y otra dirigida al personal de operaciones.

La formación dirigida al personal de mantenimiento de la plataforma, tendrá una duración mínima de 8 horas, impartida en dos días (4 horas/d x 2 dias). Se deberá estimar un número de participantes de 30 personas, las cuales se repartirán en tres grupos de 10 personas por grupo. Se explicará el hardware y software de la plataforma, las comunicaciones, los posibles problemas y cómo solventarlos, etc.

La formación dirigida al personal de operaciones y usuarios de la plataforma IIoT, tendrá una duración mínima de 32 horas impartidas en cuatro días (8 horas/d x 4 días). Se deberá estimar un número de participantes de 50 personas, las cuales se repartirán en dos grupos de 25 personas por grupo. En esta formación se explicará a los usuarios la utilización de la plataforma, el funcionamiento de la ingesta de datos, la monitorización y supervisión, las alarmas, etc.

7.1.6 Control de calidad

Antes de la aceptación de los equipos y software asociado, se harán pruebas de funcionamiento y respuesta del sistema con el objeto de demostrar las funcionalidades descritas en el punto 8.1 y subsiguientes.

El proveedor deberá realizar en su oferta una propuesta inicial de plan de pruebas para la verificación y validación final de la solución implementada.

7.2 Lote 2: Condiciones operativas en el ámbito de TI y ciberseguridad de la plataforma IIoT

7.2.1 Cobertura del servicio

El servicio de proveedor cubrirá el despliegue, estructuración, programación y puesta en marcha de los cluster y nodos descritos en el punto 8.2 y subsiguientes.

El proveedor deberá indicar en su propuesta técnica el sistema operativo de los servidores según la plataforma IIoT elegida.

El proveedor asegurará los servicios necesarios en los servidores para soportar el streaming de datos, tales como Data Paths, Pipelines, Cloud Pipelines y coordinación de los clusters.

El proveedor asegurará los servicios necesarios en los servidores para soportar el sistema de orquestación y CMDB (Configuration Management Database).

El proveedor asegurará los servicios necesarios en los servidores para soportar el sistema de observabilidad.

7.2.2 Metodología de trabajo

Se mantendrán reuniones periódicas (mínimo semanales) con los interlocutores de IIoT - IT para informar de los avances de los trabajos.

El proveedor actualizará semanalmente el estado de ejecución de los trabajos respecto a la planificación prevista.

Los interlocutores de IIoT - SCI - OT al iniciarse la ejecución del proyecto abrirán una lista de desviaciones del proyecto que se tratarán semanalmente y el proveedor propondrá soluciones y plazos de resolución.

7.2.3 Equipo de trabajo

El equipo de proyecto debe constar al menos del siguiente personal, si bien dependiendo de la fase del mismo no todo el personal debe estar dedicado a él a tiempo completo. No obstante, todo el equipo debe estar disponible para corregir las desviaciones que puedan surgir en la ejecución del proyecto.

Perfil: Un/a (1) Director de proyecto

- Formación: Titulado en ingeniería o ciencias
- Cualificación: Responsable de la gestión y la coordinación del área de desarrollos de la empresa con capacidades de asignación/desasignación de recursos dentro de su propia empresa, así como de la resolución de problemas graves que afecten al desarrollo del proyecto.
- Experiencia: Requeridos al menos CINCO (5) años de experiencia como Director de Proyecto o Jefe de Proyectos de servicios similares.

Perfil: Un/a (1) Jefe/a de proyecto

Será el responsable de la correcta ejecución de las diferentes actividades y tareas requeridas. Este perfil profesional tendrá que disponer como mínimo:

- Estudios de educación Universitària de carácter científico tecnológico como grados y/o másters en ingeniería (industrial, telecomunicaciones, informática o similar) o ciencias.
- Experiencia mínima de CINCO (5) años en la gestión de proyectos.
- Conocimientos en metodologías Agile o similares.

Perfil: Un/a (1) Técnico/a de arquitectura de sistemas

Será el responsable de la implementación técnica de las tareas requeridas en este lote. El perfil profesional tendrá que disponer como mínimo de:

- Estudios de educación Universitària de carácter científico tecnológico como grados y/o másters en ingeniería (industrial, telecomunicaciones, informática o similar) o ciencias o estudios de Técnico de Grado Superior de Formación Profesional en tecnologías de la información o similares.
- Experiencia mínima de CINCO (5) años como líder técnico en proyectos de Arquitectura de Sistemas.

- Experiencia mínima de TRES (3) años como Líder técnico, en proyectos bajo tecnologías Cloud propuestas en la solución técnica presentada y en Blob Storage, Databricks, Snowflake, Synapse.
- Conocimientos en metodologías Agile o similares.

7.2.4 Entregables

- Licencias del software instalado descrito en el punto 8.2 y subsiguientes.
- Manual detallado sobre la plataforma IIoT implementada y pruebas de validación.
- Documento con la descripción de la red, configuraciones, usuarios y claves.
- Ficheros de configuración de todos los equipos.
- Cualquier otra documentación que complemente la relación anteriormente expuesta y que se considere necesaria para la operación y mantenimiento del hardware y software implementado.

7.2.5 Control de calidad

Antes de la aceptación de los equipos y software asociado, se harán pruebas de funcionamiento y respuesta del sistema con el objeto de demostrar las funcionalidades descritas en el punto 8.2 y subsiguientes.

7.3 Lote 3: Condiciones operativas PMO

7.3.1 Cobertura del servicio

El servicio se tendrá que llevar a cabo en horario compatible con el de Aigües de Barcelona y la prestación del servicio se realizará en un tiempo medio estimado de 4-5 horas diarias, que pueden aumentar o disminuir de forma puntual dependiendo de las necesidades del trabajo, las reuniones de seguimiento etc. No hay un mínimo de horas diarias facturables, es decir, en ningún caso se facturará a Aigües de Barcelona un mínimo de horas diarias sin que estas se hayan efectuado durante el desarrollo del servicio.

Se estima un volumen total de 1.572 horas a realizar en un periodo previsto de cobertura del servicio de 24 meses, desde el inicio del proyecto hasta su finalización.

7.3.2 Metodología de trabajo

Con independencia de la metodología de proyectos utilizada, se prevé una serie de actividades básicas que se consideran necesarias para la consecución de los objetivos del servicio solicitado las cuales se describen a continuación.

Definición de requerimientos

A partir de unos requerimientos de alto nivel y en base al presupuesto de la iniciativa hay que dar soporte a la elaboración, por parte del proveedor encargado del desarrollo, de un documento detallado de análisis funcional en aquellas tareas o subtareas del proyecto que así lo requieran.

Seguimiento y coordinación del proyecto

La empresa adjudicataria deberá disponer de todas las herramientas y accesos necesarios para desarrollar sus tareas.

Deberá realizar el seguimiento de las diferentes actividades del proyecto, y que estas se ejecutan según la planificación. Convocar y coordinar las reuniones de dirección y seguimiento del proyecto, y facilitar la gestión del proyecto a los servicios técnicos de Aigües de Barcelona, coordinando a los diferentes adjudicatarios de los diferentes lotes.

Se requiere un seguimiento activo de los riesgos en los cuales pueda incurrir el proyecto, ya sean económicos, de calidad, de retraso, o de cualquier tipo. e informar de ellos inmediatamente a Aigües de Barcelona, proponiendo soluciones y alternativas de resolución.

Deberá velar por la coordinación necesaria entre todas las empresas adjudicatarias del proyecto.

Cierre del proyecto

Deberá realizar un informe de cierre con el resumen de los objetivos alcanzados y la justificación de las posibles desviaciones.

La metodología de seguimiento de proyectos dentro de Aigües de Barcelona puede ser tradicional, Agile o mixta, sin que esto pueda representar un obstáculo en la consecución de los objetivos solicitados.

7.3.3 Equipo de trabajo

El equipo mínimo que se tendrá que adscribir a la ejecución del contrato por parte del Prestador del Servicio tendrá que incluir:

Un (1) Responsable del Servicio

El adjudicatario nombrará a un Responsable global del Servicio. Este Responsable del Servicio deberá tener la capacidad, conocimientos y experiencia suficientes a los efectos de supervisar, coordinar y velar por la correcta prestación del Servicio, y ejercer labores de interlocución con Aigües de Barcelona para el seguimiento de la ejecución del Contrato. Tendrá que velar para que la estrategia seguida en la prestación del servicio esté en todo momento alineada con la necesidades establecidas en el presente pliego, controlando y garantizando que todas las decisiones y acciones que se tomen estén focalizadas en la correcta ejecución de las actividades del servicio.

Un (1) Gestor de Proyectos (PMO)

Será el responsable de la correcta ejecución de las diferentes actividades y tareas requeridas. Este perfil profesional tendrá que disponer como mínimo de:

- Estudios de educación Universitaria de carácter científico o tecnológico como grados y/o masters en ingeniería (industrial, telecomunicaciones, informática o similar) o ciencias.
- Experiencia mínima de ocho (10) años en el ámbito OT.
- Experiencia mínima de cinco (5) años como Jefe de Proyecto en el ámbito OT.
- Gestión de proyectos de manera telemática mediante herramientas colaborativas.
- Valorable experiencia en el ámbito TI y Ciberseguridad.
- Valorable experiencia en el sector medioambiental.

En cualquier caso, el perfil propuesto por el licitador tiene que contar con las competencias y habilidades mínimas necesarias para desarrollar, con garantías, las actividades definidas que permitan ofrecer la correcta prestación del servicio, a saber:

- Destreza comunicativa e interpersonal.
- Capacidad de detectar y resolver problemas.
- Alta capacidad de organización y control de la información.
- Personas activas y con iniciativa, para la mejora de los servicios.
- Orientación al trabajo en equipo.

En caso de necesidad de sustitución de algún miembro del equipo, se tendrá que asignar otra persona que disponga de la calificación requerida, y si para asegurar la permanencia del conocimiento adquirido y su transferencia fuera necesaria la concurrencia entre los recursos entrantes y salientes, durante el mencionado periodo solamente se tendrán en cuenta como horas productivas las de uno de los recursos, para cualquier contabilidad del esfuerzo.

7.3.4. Entregables

La documentación mínima que tendrá que elaborar el servicio de soporte a los proyectos según la fase en la que se encuentren es:

- Actas de las reuniones de toma de requerimientos.

- Documento de “descripción ampliada del proyecto” o funcional (requerimientos detallados).
- Planificación detallada del proyecto en curso.
- Informes de seguimiento para el Comité de Dirección.
- Plan de pruebas a ejecutar y ejecutadas.
- Informe y fichas de cierre del proyecto.
- Cualquier otra documentación para la correcta ejecución y cierre del proyecto.

7.3.5 Control de calidad

El PMO será el responsable de asegurar la calidad de todos los componentes que forman parte del proyecto.

Antes de la aceptación de las soluciones implementadas, se harán pruebas de funcionamiento y respuesta del sistema con el objeto de demostrar las funcionalidades descritas en el apartado 6.1, 6.2 y 6.3 de este documento.

Una vez validado, por Aigües de Barcelona, el plan de pruebas a realizar para cada uno de los proveedores del proyecto, el PMO será el responsable de realizar el seguimiento de las mismas y exponer los resultados así como suministrar los registros y pruebas de validación correspondientes a Aigües de Barcelona.

8 PLAZO DE ENTREGA

8.1 Planificación y plazo de entrega lote 1 (OT)

Con la oferta se deberá indicar el plazo de entrega y la planificación de los trabajos, en cualquier caso el plan de ejecución nunca deberá sobrepasar los 2 años de ejecución.

8.2 Planificación y plazo de entrega lote 2 (TI y ciberseguridad)

El plazo de entrega de todos los productos adquiridos será de un máximo de 8 semanas desde la entrada en vigor del contrato.

Una vez realizada la entrega del material, el plazo de ejecución será de un máximo de 8 semanas.

Con la oferta se entregará la planificación prevista de ejecución de los trabajos.

8.3 Planificación y plazo de entrega lote 3 (PMO)

Con la oferta se deberá indicar el plazo de entrega y la planificación de los trabajos.

9 GARANTÍA

9.1 Garantía suministros y servicios lote 1 (OT)

El hardware implementado en la plataforma IIoT en la ejecución del lote 1 tendrá la garantía del fabricante, como mínimo será de UN (1) AÑO, a partir del suministro e implementación del mismo.

El software implementado en la plataforma IIoT en este lote número 1 tendrá la garantía según las condiciones de licenciamiento del fabricante o proveedor de las mismas, como mínimo tendrá una garantía de TRES (3) AÑOS, a partir de su instalación.

Finalmente, los servicios ejecutados por el proveedor, tendrán una garantía de UN (1) AÑO, a contar desde la finalización del proyecto (entrega de la Ficha de cierre de Proyecto).

9.2 Garantía suministros y servicios lote 2 (TI y ciberseguridad)

La del hardware y licencias sistemas operativos la del fabricante y de los servicios realizados un año a partir de la aceptación de los equipos y software asociado.

9.3 Garantía servicios lote 3 (PMO)

El periodo mínimo que tendrán que tener como garantía será de SEIS (6) meses, a contar desde la finalización del contrato.

Esta garantía hace referencia a la ejecución de post-trabajos derivados de los trabajos realizados por los perfiles asociados al contrato durante la ejecución del proyecto. Durante el periodo de garantía se podrá requerir la corrección de errores detectados en los entregables del proyecto.

10 GESTIÓN DEL SERVICIO

10.1 Dirección del Servicio

La coordinación, seguimiento, control y valoración de la ejecución del servicio, así como de los encargos asociados al objeto del contrato, o de ampliaciones o modificaciones establecidas por Aigües de Barcelona, para el correcto cumplimiento del contrato y correcta ejecución del servicio irán a cargo del Director/a del Servicio (en adelante la DS). Así mismo, ésta podrá designar a otra/s persona/s del servicio técnico de Aigües de Barcelona que considere y que a tal efecto tendrán las facultades delegadas.

Para poder cumplir con la máxima eficiencia y efectividad su misión, la DS gozará de las más amplias facultades, debiendo conocer y participar en todas aquellas actuaciones que se realicen por el adjudicatario.

Las instrucciones u órdenes que supongan modificaciones o alteraciones sobre la programación o los importes económicos sólo podrán ser dictadas y aprobadas por la DS mediante comunicación escrita.

El prestador del servicio estará obligado a seguir las instrucciones referentes a la tipología, orden, modo y tiempo de ejecución de los trabajos que puedan ser comunicadas por la DS, quien supervisará y evaluará el cumplimiento de los trabajos objeto del servicio y los niveles de calidad, el cumplimiento de la normativa y los criterios establecidos, así como cualquier otra prescripción de la prestación del servicio.

En caso de incumplimiento por parte del prestador del servicio, la DS podrá encargar los trabajos necesarios a otra empresa con cargo al contratista, sin perjuicio de otras responsabilidades.

Las funciones de la DS, a título indicativo y no exhaustivo, serán las siguientes:

- Velar por el cumplimiento del contrato y de los objetivos del proyecto.
- Impulsar la programación y ejecución de las actuaciones del plan de trabajo definido objeto del servicio.
- Asistir al operador económico para la implantación del plan de trabajos, a fin de que se mantengan las condiciones de funcionalidad, estabilidad, seguridad y calidad previstas en la documentación contractual.
- Aprobar la programación de los trabajos y modificarla si lo considera oportuno.
- Dirigir los trabajos objeto del contrato y dar las instrucciones que se consideren oportunas.
- Validar la información técnica elaborada así como todos aquellos otros documentos que solicite la DS y sean entregados por el prestador del servicio.
- Aprobar las certificaciones de los trabajos realizados.

- Establecer los controles de calidad y comprobaciones de los distintos aspectos del servicio y evaluar que se ejecute con las condiciones prescritas.
- Seguimiento de los indicadores de evaluación de calidad del servicio.
- En caso de incumplimiento, requerir al prestador del servicio la corrección de los trabajos si lo estima conveniente o los aspectos del incumplimiento.

10.2 Responsable del Contrato

Para cada uno de los lotes, se designará por parte del adjudicatario una persona Responsable del Contrato (en adelante la RC). La RC será la persona que tendrá la visión completa del contrato y será el principal interlocutor con Aigües de Barcelona. Entre sus funciones destacan las siguientes:

- Garantizar la rápida resolución y priorización de las incidencias graves.
- Asegurar el cumplimiento de la planificación general y de los compromisos del contrato en los diferentes aspectos.
- Actuar como interlocutor principal para la gestión de las modificaciones al alcance del contrato que puedan surgir.
- Asistencia a las reuniones de seguimiento del contrato.

10.3 Jefe/a de Proyecto

Para cada uno de los lotes, el adjudicatario designará una persona como Jefe/a de Proyecto (JP). La JP será la persona física designada expresamente por el contratista y aceptada por Aigües de Barcelona, responsable de la correcta realización del servicio y de la ejecución de los trabajos que forman parte de él, y cumplir y hacer cumplir los requerimientos, instrucciones y normativas que los regulan, con facultades suficientes para ostentar la representación del prestador del servicio, cuando sea necesaria su actuación o presencia en orden de ejecución y buena marcha de los trabajos, por los que deberá acreditar la capacidad, experiencia y titulación suficiente con la finalidad de dirigir y organizar la ejecución del servicio.

Todo el personal adscrito al servicio y trabajos objeto del contrato dependerá jerárquicamente del mismo a efectos de ejecución del contrato.

Serán los interlocutores con los responsables técnicos de Aigües de Barcelona durante la ejecución del proyecto objeto del contrato.

Asistirán a las reuniones de Seguimiento Operativo del proyecto.

10.4 Comités de Seguimiento

10.4.1 Comité de Seguimiento del Contrato

Se establecerá un Comité de Seguimiento del Contrato que se reunirá con carácter periódico bimestral o con la frecuencia superior que razonablemente se considere necesaria o después de TRES (3) días laborables tras una petición de cualquiera de las partes.

El Comité de Seguimiento estará compuesto por las personas que el Prestador del Servicio del lote 1 y del lote 2 (al menos, el Responsable del Contrato) y Aigües de Barcelona designen por cada parte.

En cualquier caso, el Comité de Seguimiento del Contrato será informado de la evolución del proyecto.

Las funciones del Comité de Seguimiento del Contrato serán:

- Presentación por parte del Prestador del Servicio del informe de seguimiento de los diferentes Servicios.
- Seguimiento global del proyecto.
- Aprobación de los Acuerdos de Nivel de Servicio (ANS).
- La revisión del cumplimiento de los correspondientes indicadores de nivel de servicio y el ajuste de dichos indicadores a la realidad, así como el establecimiento de las acciones correctivas si fuera necesario para su cumplimiento.
- El análisis y resolución de las incidencias o discrepancias que puedan surgir en la prestación del servicio, que no hayan podido ser resueltas en el Comité de Seguimiento Operativo.
- Cualquier cuestión relacionada con la variación del alcance del servicio.
- El análisis de cualquier modificación o adaptación del Contrato, de conformidad con aquellas que se han previsto de forma expresa en las condiciones particulares del Pliego (PCP) o bien aquellas consideradas sobrevenidas.
- Cualesquiera otras funciones que se consideren para el cumplimiento de los objetivos del Proyecto.

De las reuniones, se levantará acta por parte del adjudicatario del lote 2 según modelo del anexo 8.

10.4.2 Comité de Seguimiento del Proyecto

Se establecerá un Comité de Seguimiento Operativo que mantendrá reuniones de seguimiento, con carácter periódico semanal o con la frecuencia superior que razonablemente se considere necesaria en función de la evolución del proyecto, así como revisiones técnicas, entre el equipo de coordinación de Aigües de Barcelona y el Responsable del Servicio designado por el

Prestador del Servicio y con la parte del equipo de proyecto cuya participación se considere necesaria.

A continuación, se indican de forma no exhaustiva ni limitativa, las tareas de este Comité de Seguimiento Operativo:

- Reunión de arranque de proyecto (Kickoff).
- Reuniones de seguimiento de desarrollo (periodicidad semanal)
- Tratamiento de los Informes de Seguimiento.
- Aprobación de la Planificación del proyecto.
- Aprobación de análisis funcionales y técnicos.
- Aprobación del Plan de Pruebas y del Plan de Implantación.
- Aprobación cierre de proyecto.
- Elevar al Comité de Seguimiento del Contrato posibles riesgos o cambios significativos que impacten en el alcance del proyecto.
- Etc.

En cualquier caso, se organizarán tantas sesiones de trabajo, o las reuniones que sean necesarias para asegurar la correcta coordinación y correcta consecución de los objetivos del proyecto a desarrollar e implantar.

Se solicita a los licitadores que detallen en su propuesta la metodología concreta que proponen utilizar en la gestión del proyecto, incluyendo la especificación de procedimientos, reuniones, periodicidades, mecanismos de control y seguimiento, etc.

De las reuniones, se levantará acta por parte del adjudicatario del lote 2 según modelo del anexo 8.

11 SUBCONTRATACIÓN

Ninguna parte de las actuaciones a realizar por el adjudicatario podrá ser subcontratada sin la autorización expresa de los servicios técnicos de AB si esta no ha sido considerada previamente en la oferta del licitador y conforme a lo establecido en el PCA.

Las solicitudes para ceder cualquier parte del contrato deberán formularse por escrito y acompañarse de la documentación que acredite que la organización que debe encargarse de la realización de los trabajos objeto del subcontrato, está capacitada y equipada para su ejecución, y adjuntando la documentación técnica que, a juicio de los servicios técnicos de AB sea necesaria para garantizar la ejecución y calidad exigida en este Pliego.

Los servicios técnicos de AB tendrán una relación completa, facilitada por el adjudicatario, de todos y cada uno de los subcontratistas que han trabajado, trabajan o pueden trabajar en las actuaciones objeto de este Pliego. La aceptación del subcontrato no rebajará al adjudicatario su responsabilidad contractual. Se estará sujeto además a todas aquellas cláusulas administrativas particulares que se establezcan en el contrato.

Asimismo, el prestador del servicio facilitará al subcontratista la información que se estime necesaria en relación con las condiciones de ejecución de las actuaciones subcontratadas, aplicando en cualquier caso las mismas reglas de confidencialidad de la información que rigen al contratista y será responsabilidad de aquél velar por su cumplimiento.

12 SEGURIDAD Y SALUD LABORAL

El Prestador del servicio deberá cumplir en todo momento con la legislación vigente de prevención de riesgos laborales y seguir las indicaciones de los servicios técnicos de Aigües de Barcelona en materia de seguridad y salud laboral, así como sus procedimientos.

El Prestador del servicio deberá informar de inmediato de cualquier incidente o accidente de seguridad y salud laboral, en centros de trabajo de Aigües de Barcelona y en el ámbito de ejecución del proyecto, a los servicios técnicos de Aigües de Barcelona.

En cualquier caso, el Prestador del servicio deberá dar cumplimiento a todo lo establecido en el Pliego de Seguridad y Salud Laboral que forma parte de los documentos del contrato.

13 OTROS REQUERIMIENTOS Y SEGUIMIENTO PERTE

13.1 Entregables

Los descritos en los puntos 7.1.4, 7.2.4, 7.3.4 y 7.4.4., los cuales se resumen en la siguiente tabla:

LOTE 1	1. Esquemas eléctricos: nuevas instalaciones y modificadas. 2. Listado de materiales instalados: marca, modelo y fabricante.. 3. Tabla de conexiones UTP y eléctricas en cada instalación. 4. Reportaje fotográfico final de las instalaciones.. 5. Documentación del fabricante: manuales de instalación y mantenimiento, certificados de garantía, licencias, servicio de representación y asistencia técnica. 6. Memoria detallada plataforma IIoT y pruebas de validación. 7. Manual de operación de la plataforma IIoT, monitorización y supervisión, alarmas, cuadros de mando, etc. 8. Documento con la descripción de la red, configuraciones, usuarios y claves. 9. Ficheros de configuración.. 10. Listado de licencias del software instalado. 11. Otra documentación complementaria..
LOTE 2	1. Licencias del software instalado. 2. Manual detallado sobre las plataformas implementadas y pruebas de validación. 3. Lista de materiales instalados (Excel) con referencias del fabricante y cantidad instalada. 4. Esquema detallado del armario indicando todos los elementos instalados. 5. Fotos finales de la instalación, de los alrededores de los racks de securización, su interior y exterior, así como de los firewalls OT y sus alrededores. 6. Manuales de instalación y mantenimiento, certificados de garantía, licencias y servicio de representación y asistencia técnica. 7. Documento con la descripción de la red, configuraciones, usuarios y claves. 8. Ficheros de configuración de todos los equipos. 9. Cualquier otra documentación que complemente la relación anteriormente expuesta y que se considere necesaria para la operación y mantenimiento del hardware y software implementado.
LOTE 3	1. Actas de las reuniones de toma de requerimientos. 2. Documento de “descripción ampliada del proyecto” o funcional (requerimientos detallados). 3. Planificación detallada del proyecto en curso. 4. Informes de seguimiento para el Comité de Dirección. 5. Plan de pruebas a ejecutar y ejecutadas. 6. Informe y fichas de cierre del proyecto. 7. Cualquier otra documentación para la correcta ejecución y cierre del proyecto.

La documentación generada durante la ejecución del contrato es propiedad exclusiva de Aigües de Barcelona, sin que el Adjudicatario pueda conservarla, ni obtener copia de la misma o facilitarla a terceros. Así, el Adjudicatario tendrá que suministrar a Aigües de Barcelona la documentación derivada de la propia gestión del proyecto. Esta documentación será revisada y tendrá que ser aprobada por el personal de Aigües de Barcelona.

13.2 Acciones formativas

El proveedor deberá proponer el contenido de la formación al equipo encargado de la explotación de la solución desplegada, indicando el tiempo estimado. Será coordinado con Aigües de Barcelona la planificación de esta formación pudiéndose fraccionar en función de las necesidades.

En particular, se realizará una formación de la infraestructura IIoT por el adjudicatario del lote 1 dirigida al personal de mantenimiento y explotación de la infraestructura, en la que se abordará el funcionamiento de la solución implementada, flujos de información, actividades de mantenimiento y principales incidencias y alternativas.

Se realizará también una formación sobre el sistema de información dirigida a responsables técnicos de las instalaciones para conocer la descripción funcional del sistema de información, aplicaciones de la información, visualización e interconexiones con otros sistemas, etc.

13.3 Ubicación

Los servicios de los adjudicatarios se prestarán principalmente en modalidad mixta, desde los centros de trabajo de Aigües de Barcelona donde se realizará la instalación del hardware y el software de la plataforma IIoT; y desde las propias oficinas del adjudicatario, aquellas tareas que pueden ejecutarse a distancia.

No obstante, se darán situaciones que requieran de la presencia en las propias oficinas de Aigües de Barcelona, por motivo de asistencia a reuniones, seguimiento del proyecto, puestas en común, etc.

Corresponde a los diferentes proveedores realizar una estimación del tiempo de su equipo en modalidad presencial en los centros de trabajo de Aigües de Barcelona y en modalidad de trabajo a distancia; sin que variaciones respecto a la estimaciones realizadas por el proveedor puedan suponer un incremento en el coste de los servicios.

13.4 Recursos Materiales

Los Prestadores del Servicio de cada uno de los lotes serán responsables de disponer del equipo de trabajo y del equipamiento Hardware y Software necesario para la ejecución de las prestaciones contratadas. En ningún caso se podrá facturar la compra, suministro o instalación de equipos y recambios que sean necesarios para realizar los servicios objeto de este contrato.

No obstante lo anterior, Aigües de Barcelona proporcionará a los Prestadores de Servicios las herramientas siguientes:

- Usuarios locales o de dominio con los permisos necesarios.
- Herramientas de reporting y seguimiento del proyecto e incidencias.

El adjudicatario tendrá que utilizar las herramientas (Jira o similares) de Aigües de Barcelona para el reporting y seguimiento de las incidencias detectadas:

- En fase de definición, pruebas de aceptación y puesta en marcha, tendrán que hacer uso de las herramientas corporativas existentes en ese momento.
- En fase de implantación (parcial o total), además, tendrán que hacer uso de la herramienta de ticketing utilizada por Aigües de Barcelona en ese momento.

El acceso del Prestador del Servicio a los sistemas de información de Aigües de Barcelona se realizará mediante conexión VPN Lan-to-Lan o con usuarios VPN nominales.

El personal externo que deba trabajar en el servicio tendrá usuario personalizado en los sistemas necesarios. A este efecto se tendrá que proporcionar al inicio del servicio el nombre, apellidos y el DNI/NIE.

13.5 Registro, control y resolución de incidencias

El adjudicatario de cada lote deberá llevar un registro de las incidencias detectadas, los cuales se ubicarán en accesos compartidos indicados por los responsables técnicos de Aigües de Barcelona.

El adjudicatario de cada lote estará obligado a plantear las acciones necesarias para su resolución, las cuales serán consensuadas y validadas con los responsables técnicos de Aigües de Barcelona. Estas acciones quedarán registradas en el registro de incidencias. Así mismo, deberán reportar en el mismo el avance y estado de las acciones.

La frecuencia y contenidos de estos reportes serán consensuados por ambas partes en la fase correspondiente. Estos procedimientos pueden ser cambiados en cualquier momento por Aigües de Barcelona, previa comunicación y aceptación por parte del adjudicatario, quién se compromete a adoptarla en el plazo máximo que se establezca.

Cada incidencia vendrá informada con una prioridad (alta, media o baja). En cualquier caso, la totalidad de las incidencias deberán ser resueltas dentro del período de proyecto y garantía.

En caso necesario, se solicitará soporte presencial para la resolución de las incidencias.

Así mismo, en el caso de que Aigües de Barcelona lo considere necesario, solicitará un informe de estado de resolución de las incidencias generadas.

Se considerará resuelta la incidencia cuando en el entorno de pruebas, se haya realizado el despliegue del correctivo y comprobado que funciona. No obstante, la incidencia no se cerrará hasta que se haya desplegado en el entorno de producción y validado que funciona correctamente.

13.6 Acceso

El acceso del Prestador del Servicio a los sistemas de información de Aigües de Barcelona se realizará mediante conexión VPN Lan-to-Lan o con usuarios VPN nominales.

Todo el personal externo que tenga que trabajar en el servicio tendrá usuario personalizado en los sistemas necesarios. A tal efecto se deberá proporcionar al inicio del servicio el nombre, apellidos y DNI/NIE de los mismos.

13.7 Idioma

El proyecto se deberá prestar a nivel comunicativo en castellano y/o catalán tanto hablado como escrito para una fluida comunicación con técnicos de Aigües de Barcelona y con los usuarios. Este apartado aplica igual para los adjudicatarios de todos los lotes.

14. SEGURIDAD DE LA INFORMACIÓN

Tanto los Prestadores del Servicio, como sus trabajadores, deberán respetar y seguir las normas y regulaciones internas que dicte el área de Seguridad de la Información, en materia de Seguridad de la información y uso de las TIC, como mínimo:

- Aceptar las normas establecidas en el área de Seguridad de la Información tanto en el momento de su incorporación como después de cada cambio importante de las políticas, normas o regulaciones (ver anexo 1).
- Dar cumplimiento a todas las normas, políticas y marcos reguladores vigentes durante el periodo del contrato.
- Permitir y facilitar la realización de auditorías de cumplimiento de las normativas establecidas para Seguridad de la Información, internas o externas, sobre los sistemas de información vinculados a la prestación del Servicio, y garantizar la posibilidad de trazabilidad de las acciones realizadas por el auditor para facilitar el seguimiento de las mismas así como sus posibles impactos no deseados.

A la finalización del contrato, el Prestador del Servicio quedará obligado a la entrega o destrucción en caso de ser solicitada, de cualquier información obtenida o generada como consecuencia de la prestación del servicio.

ANEXOS

Anexo 1: Normas de seguridad IT de Aigües de Barcelona (.pdf)

Anexo Nº 4

"NORMAS DE SEGURIDAD IT DE AIGÜES DE BARCELONA"

ÍNDICE

1. Objeto e introducción del documento

2. Intercambio de información y software SI-N-07-02/01

3. Configuración y administración segura

3.1 Configuración segura

3.2 Administración segura

4. Identificación y autentificación de usuarios

5. Identificación de usuario

6. Gestión de contraseñas y credenciales de clientes

7. Comunicación de los incidentes de seguridad

1. Objeto e introducción del documento

El objeto del presente documento es establecer la normativa de seguridad en la gestión de los Sistemas de Información de Aigües de Barcelona (AB) y en la identificación, autentificación de usuarios y gestión de las contraseñas de acceso a los mismos.

2. Intercambio de información y software SI-N-07-02/01

El intercambio de información o software calificados como de uso interno, restringido o confidencial que realice AB con otras organizaciones, debe estar formalizado en acuerdos, validados por la Dirección Jurídica, que deben establecer las condiciones en las que se realizarán dichos intercambios.

Cuando, por razones de urgencia y eficiencia del servicio, sea imposible la formalización previa de dicho acuerdo, el intercambio de información estará sujeta a las condiciones generales previstas en esta norma y será el remitente el responsable de su cumplimiento.

El intercambio debe realizarse respetando la clasificación y el etiquetado de la información que se maneje durante dicho intercambio.

Los intercambios de información clasificada como restringida, así como de datos de carácter personal de nivel alto, se deben realizar empleando mecanismos de cifrado que impidan la divulgación no autorizada.

En los acuerdos se deben establecer los mecanismos oportunos para facilitar la gestión de estos intercambios y plasmar las responsabilidades y obligaciones legales cuando se lleven a cabo, especialmente las relacionadas con los datos de carácter personal.

Estos acuerdos deben indicar las responsabilidades de control y notificación del envío, transmisión y recepción de la información que se intercambia. Se debe asignar un gestor para cada acuerdo con la responsabilidad de controlar y hacer un seguimiento de su desarrollo.

En el ámbito legal, los acuerdos deben establecer las responsabilidades y obligaciones legales relativas al intercambio, especialmente aquellas derivadas del intercambio de datos de carácter personal con otras entidades, cesionarias o cedentes, de acuerdo con la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD) y con el Reglamento de Desarrollo de la LOPD. No se podrán realizar intercambios de aquella información clasificada como confidencial.

Es responsabilidad de la Dirección de Seguridad TI identificar los mecanismos especiales requeridos para proteger activos críticos, como los de cifrado indicados anteriormente o el empleo de soluciones de no-repudio, con la finalidad de asegurar la recepción de la información por parte del destinatario.

3. Configuración y administración segura

3.1. Configuración segura

Todos los sistemas deberán estar configurados para verificar la identidad de los usuarios que acceden a ellos, de modo que no se comprometan las credenciales de autentificación y se garantice su identificación unívoca.

Asimismo, en función del perfil de los usuarios y la información que el sistema procese, se deberá determinar la asignación de privilegios y los servicios habilitados en cada caso. La configuración y asignación de privilegios debe regirse por el principio de menor privilegio, limitando los permisos únicamente a los estrictamente necesarios para la operativa diaria de trabajo de los usuarios. En este sentido, únicamente los administradores y operadores de los sistemas de información deben tener acceso a las utilidades de gestión y administración del

sistema que requieren para el ejercicio de sus funciones, y pueden existir distintos niveles de derechos de administración.

Se deberán limitar los servicios de red abiertos en los diferentes sistemas de información. La configuración de los servicios de red activos debe regirse por el siguiente principio: "Se prohíbe todo aquello que no se encuentra explícitamente permitido", o lo que es lo mismo, se deben desactivar todos los servicios de red que se activan por defecto durante la instalación y cuyo uso no se encuentra motivado por una necesidad de negocio u operativa clara.

Adicionalmente, para evitar, en la medida de lo posible, la exposición a ataques de denegación de servicio, los dispositivos y elementos de comunicaciones deberán estar adecuadamente configurados mediante el establecimiento de medidas de protección como podrían ser:

- Limitaciones en el tiempo máximo de vida de conexiones inactivas.
- Limitaciones en el número máximo de conexiones abiertas.
- Restricciones en los algoritmos de propagación de información de encaminamiento.

Asimismo, en aquellos elementos de comunicaciones que provean acceso a la red de comunicaciones de Agbar o que utilicen algoritmos de encaminamiento dinámicos, deberán emplearse mecanismos de autentificación mutua basados en claves precompartidas, certificados digitales u otros mecanismos que proporcionen mayor seguridad.

Por último, los sistemas de información deberán estar configurados para registrar todos aquellos eventos que sean necesarios para asegurar la trazabilidad de las acciones realizadas en el sistema, con especial atención a los ficheros clasificados como de nivel alto según la LOPD.

3.2. Administración segura

La administración remota de los sistemas de información debe ser realizada por medio de herramientas y/o protocolos de administración que provean medios para identificar unívocamente al usuario administrador y para que las credenciales de dicho usuario administrador viajen cifradas por la red de comunicaciones empleando técnicas criptográficas.

Asimismo, se limitará el tiempo máximo de conexión de los usuarios administradores para evitar que las sesiones permanezcan abiertas de manera indefinida, lo que facilitaría la captura de sesiones por parte de usuarios no autorizados.

Incluido en los procesos de administración de sistemas, se deberá llevar a cabo un proceso de revisión periódica de ficheros temporales en servidores centrales y sistemas de información de Agbar, que corrija posibles fallos ocurridos durante el proceso de borrado de ficheros temporales. El tratamiento de estos ficheros temporales se debe ajustar a lo dispuesto en las normativas legales vigentes en materia de protección de datos de carácter personal (LOPD).

4. Identificación y autentificación de usuarios

Todos los sistemas de información no públicos de las unidades y sociedades operativas de AB deberán disponer de mecanismos que verifiquen la identidad de los usuarios que los usan, de tal forma que se restrinja los recursos a los que debe acceder cada usuario.

Los usuarios dispondrán de un único identificador para todos los sistemas de información, permitiendo determinar las operaciones que pueda realizar en los distintos sistemas a través de su identificador, salvo las excepciones reflejadas en el apartado “Identificador de usuario”.

El mecanismo de autentificación de cada sistema se podrá implantar mediante:

- Software de control de acceso inherente al propio sistema.
- Herramienta de software de control de acceso agregado al sistema.

La autentificación, normalmente, se realizará mediante el empleo de contraseñas siguiendo los criterios de robustez de contraseñas indicados en el apartado de "Gestión de contraseñas y credenciales".

Todos los mecanismos de autentificación deberán ser supervisados por la Dirección de Seguridad TI, que verificará la correcta parametrización de la normativa de seguridad relativa a la autentificación de usuarios.

La autentificación en el sistema deberá garantizar que el usuario sólo tenga acceso a los recursos que necesite para el desempeño de sus funciones, no disponiendo de permisos de acceso a las herramientas propias del sistema, salvo que las necesite para el desarrollo de sus funciones (por ejemplo, administradores de sistemas).

En los procesos de autentificación a través de redes se evitará la transmisión de la clave de acceso de modo legible. Cuando el usuario acceda al sistema se le deberá mostrar, si es posible, la fecha y hora de su último acceso. Este aviso puede alertar al usuario de la existencia de accesos no autorizados. En este caso deberá de comunicarlo inmediatamente al Jefe de Seguridad de la Información de la entidad a la que pertenezca.

Cuando la criticidad del servicio o recurso lo requiera, la Organización de Seguridad de la Información promoverá el uso mecanismos de autentificación basados en infraestructura de clave pública (PKI) y almacenamiento de claves en dispositivos externos (SmartCards, E-Tokens, etc.) Cuando se necesite acceso a archivos o transacciones especialmente sensibles el usuario debe ser re-autenticado, en caso de que sea posible técnicamente.

Con el fin de evitar el acceso no autorizado, el proceso de identificación y autentificación de usuarios, deberá estar dotado de controles para el bloqueo automático del identificador de usuario y su inhabilitación temporal para el acceso al sistema en los siguientes casos:

- Por número de intentos de acceso incorrectos.
- Por inactividad del usuario en el sistema.

En estas situaciones, y en cualquier otra originada por el bloqueo de un identificador de usuario, el propio usuario deberá solicitar formalmente, a través del correo electrónico corporativo, la rehabilitación de sus privilegios de usuario. En el caso de que el identificador de usuario bloqueado sea el de correo electrónico, el superior jerárquico del usuario implicado deberá solicitar, por los procedimientos establecidos, la rehabilitación de los privilegios del mismo. Tanto si el desbloqueo se realiza manual como automáticamente deberán implantarse controles que permitan identificar y detectar intentos de acceso no autorizados.

Con el objetivo de evitar ataques de denegación de servicio a los usuarios administradores, los identificadores de usuarios administradores no se bloquearán. Se deberán establecer los controles compensatorios adecuados para monitorizar intentos fallidos de inicio de sesión para dichos usuarios, así como el aumento de tiempo para reintentos o bloqueos temporales, siempre que sea técnicamente posible.

5. Identificación de usuario

El acceso a cualquiera de los sistemas de información de AB se realizará utilizando un identificador de usuario convenientemente autorizado ([UserID]). El identificador de usuario deberá estar asignado a una persona física y tendrá carácter personal e intransferible. Consecuentemente, y asociado a cada identificador asignado a una persona física, se conservarán los datos que, como mínimo, permitan relacionar unívocamente el identificador de usuario con la persona física.

La nomenclatura del identificador de usuario se construirá con independencia de la función desempeñada por el usuario, de su puesto de trabajo, del departamento al que pertenece y del sistema al que se conecta. El identificador de usuario permanecerá asociado a su propietario de

AB con independencia de los cambios de destino o de categoría que pudiera tener o, incluso de baja; y de acuerdo a la legislación vigente en materia de protección de datos de carácter personal.

Las personas que no pertenecen a la plantilla de trabajadores de AB deben recibir identificadores que sigan los mismos procesos de aprobación que para los nuevos empleados. Los derechos de acceso de los usuarios que no pertenecen a AB deben de otorgarse sólo por el periodo de tiempo estrictamente necesario y deberán ser reevaluados periódicamente.

No estará permitida la creación o utilización de usuarios genéricos salvo en aquellos casos en los que sea estrictamente necesario por razones operativas, funcionales, etc., que, por su naturaleza, aconsejan u obligan al uso de los mismos y previa autorización específica del Jefe de Seguridad de la Información de la entidad correspondiente. En estos casos, se extremará el seguimiento de las actividades realizadas con el usuario genérico, asegurando que se conoce, en todo momento, el grupo de usuarios que lo emplean. Cuando la necesidad de emplear el usuario genérico por un usuario del grupo finalice, se deberá modificar la contraseña de acceso compartida para hacer efectiva la salida de dicho usuario del grupo e impedir el empleo del usuario genérico más allá de sus necesidades.

Asimismo, salvo en situaciones justificadas por el desempeño de las funciones, cada persona física tendrá asociado un único identificador de usuario. Como excepción, un usuario podrá disponer de más de un identificador de usuario en caso que los privilegios asignados a cada uno sean distintos y técnicamente no sea posible recoger todos los privilegios en un sólo identificador de usuario o no sea recomendable mantener todos los privilegios en un único identificador de usuario por cuestiones de seguridad.

6. Gestión de contraseñas y credenciales de clientes

Para evitar la posible averiguación de las contraseñas por parte de terceros, éstas deberán cumplir una serie de requisitos a la hora de la generación de las mismas.

Como pauta general, las contraseñas de usuarios no deberán tener una longitud inferior a 6 (seis) caracteres alfanuméricos, incluyendo al menos dos caracteres numéricos y dos alfabéticos.

Para evitar la selección de contraseñas fácilmente adivinables, cuando sea tecnológicamente posible, los sistemas de control de acceso dispondrán de una colección de reglas de sintaxis que impedirán, por ejemplo, que la contraseña coincida con el identificador de usuario, o corresponda a una secuencia de longitud válida de un mismo carácter repetido, coincida con blancos o constituya una palabra conocida. Esta verificación se ejecutará de manera automática durante el proceso de cambio de contraseñas en las aplicaciones o herramientas en las que se utilice.

Los sistemas deben permitir al usuario el cambio de su contraseña de forma autónoma cuando éste lo estime oportuno. Asimismo, cuando se acceda por primera vez a un sistema o cuando se haya solicitado, a través de los procedimientos establecidos a tal efecto, una rehabilitación o desbloqueo de la contraseña, el sistema de control de acceso obligará al usuario al cambio de la misma en su primer acceso. La contraseña inicial deberá ser generada de manera aleatoria.

Los usuarios podrán solicitar, siguiendo los procedimientos establecidos, el desbloqueo de su identificador o un cambio de contraseña cuando no la recuerden o tengan sospecha de que ha perdido el carácter de secreta y no dispongan de la opción para cambiarla o desconozcan cómo realizar el cambio.

Después de cinco intentos fallidos consecutivos en la introducción de la contraseña por parte del usuario, como máximo, el sistema deberá deshabilitar el identificador asociado hasta su inicialización o desbloqueo.

Los sistemas de información de AB deberán disponer de mecanismos de control de acceso que permitan:

- Restringir, individualizar, registrar, controlar y, eventualmente, bloquear el acceso a la información y a las aplicaciones.
- Proteger la información y las aplicaciones de accesos realizados por personal no autorizado.
- Autenticar a todos los usuarios antes de que éstos accedan a cualquiera de los recursos de uso interno, restringido o confidencial para los que estén autorizados.
- Impedir la existencia de identificadores de usuario sin contraseña asignada.
- Proteger las contraseñas de los usuarios del siguiente modo:
    - Almacenando el resumen o "hash" generado con algoritmos estándar de cifrado.
    - No mostrarse en pantalla en texto claro
    - Restringir a todos los usuarios, en la medida de lo posible, la posibilidad de establecimiento de sesiones concurrentes.
    - Finalizar sesiones por inactividad durante un tiempo determinado. Se establecerá 5 minutos como valor de referencia, aunque deberá ser configurable en función de la criticidad y sensibilidad de los datos que se manejen.
    - No permitir la visualización de información referente al sistema hasta que el proceso de inicio de sesión haya terminado satisfactoriamente.
    - No permitir el almacenamiento de contraseñas en programas, "scripts" o códigos desarrollados para conexión automática a los sistemas de información. Salvo excepciones previamente autorizadas por la Dirección de Seguridad TI. La Dirección de Seguridad TI deberá definir mecanismos de control de acceso alternativos que efectúen controles no cubiertos por los sistemas de control de acceso instalados en los entornos, así como evaluar las ventajas y debilidades de las nuevas versiones y/o productos alternativos o complementarios.

La Dirección de Seguridad TI deberá evaluar los mecanismos de autenticación disponibles alternativos a las contraseñas, por ejemplo, biométricos, tarjetas, tokens, etc. para aquellos sistemas donde se requiera un nivel de autenticación más seguro.

7. Comunicación de los incidentes de seguridad

En caso de detección de un incidente grave de seguridad (mediante sistemas de detección de intrusiones, análisis de logs, comunicación de un tercero, alarmas de seguridad, etc.), la Dirección de Seguridad AB deberá ser informada a la mayor brevedad posible a través de líneas de comunicación que se establecerán previamente con éste propósito.

La Dirección de Seguridad se encargará de iniciar un informe hacia las figuras, escogidas entre aquellas que previamente habían sido identificadas, cuya participación sea necesaria en la resolución del incidente. Esta elección se hará en función de la criticidad del incidente, el grado de conocimiento necesario o los sistemas a los que afecte.

Las Áreas de Asuntos Legales (Dirección Jurídica) y Recursos Humanos deberán ser informadas en caso de que el incidente necesite tomar acciones disciplinarias o legales y en caso de que pueda tener repercusiones legales para AB.

Se deberán reportar aquellos incidentes significativos a los niveles jerárquicos superiores establecidos con la finalidad de obtener autorizaciones o de informar sobre la actuación de AB frente a incidentes de seguridad.

El reporte de información sobre incidentes de seguridad quedará restringido únicamente a aquellas personas absolutamente necesarias. Cualquier divulgación de dicha información deberá ser autorizada por la Dirección de Seguridad.

Es responsabilidad de la Dirección de Seguridad mantener un registro con los datos de aquellas personas que han sido informadas de cada incidente con la finalidad de detectar una posible divulgación no autorizada.

Tanto los empleados de las entidades de AB como los trabajadores de empresas externas conocerán las líneas de reporte de incidentes de seguridad y tienen el deber de utilizarlas en caso de detectar un incidente de seguridad. Si la persona que detecta el incidente no está segura de si se trata de un incidente o no, deberá reportarlo igualmente.

Anexo 2: Seguridad en sistemas OT (.pdf)

GUÍA SOBRE CONTROLES DE SEGURIDAD EN SISTEMAS OT

MINISTERIO DEL INTERIOR

SECRETARÍA de ESTADO de SEGURIDAD

GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

En el mes de julio de 2020 se solicitó la colaboración de organismos públicos, empresas privadas y del sector académico con la finalidad de identificar las carencias de seguridad en los sistemas de operación, así como la definición de las medidas compensatorias que podrían subsanar dichas carencias.

En concreto, las entidades que han colaborado con sus respuestas son las siguientes:

ASOCIACIONES/FUNDACIONES	CCI
	Fundación Borredá
	Instituto El Cano
	ISACA
CONSULTORAS	Deloitte
	EY
	GMV
	Grupo SIA-INDRA
	Ecix
	Capgemini
EMPRESAS	Enigmedia
	Aiuken Solutions
	NextVision
	Agbar
	Ingenia
	Entelgy Innotec Security
FABRICANTES	Check Point Software Technologies
	Tecnalia/PESI
	Siemens
UNIVERSIDADES	Universidad Pontificia Comillas
	Universidad de Málaga
COORDINACIÓN	ISMS Forum
	Oficina de Coordinación de Ciberseguridad

CONTENIDO

1. INTRODUCCIÓN Y CONTEXTO ACTUAL **5**

1.1 Introducción

1.2 Safety & Security

1.3 Redes OT e ICS

1.4 Seguridad en la cadena de suministro

1.5 IoT & Privacidad

2. MARCO REGULATORIO **11**

3. RECOMENDACIÓN DE MEDIDAS BÁSICAS DE SEGURIDAD **16**

3.1 Gestión de la ciberseguridad en Sistemas de Control Industrial (SCI)

3.2 Medidas básicas recomendadas

4. RESULTADOS OBTENIDOS **25**

ANEXO I - RESULTADOS DE LA CONSULTA 26

ANEXO II - ESTADÍSTICAS 52

ANEXO III - ADAPTACIÓN DE LAS AMENAZAS DEL CATÁLOGO MAGERIT A ENTORNOS OT 57

ANEXO IV - GLOSARIO DE TÉRMINOS 63

1. INTRODUCCIÓN Y CONTEXTO ACTUAL

1.1 Introducción.

Sin lugar a dudas las tecnologías de la información y las comunicaciones (TIC) hoy soportan la gran mayoría de los servicios que se prestan a nivel mundial. Persisten muy pocos servicios esenciales para el ser humano cuyo correcto funcionamiento no dependa de las tecnologías de la información.

Esto se está produciendo a gran velocidad de cambio y es consecuencia de la búsqueda de la eficiencia en todos los sectores. En los últimos años estos procesos de cambio tienen como vehículo conductor los programas de transformación digital, en los que prácticamente toda institución está inmersa. El actual escenario hará que esa dependencia de la Tecnologías de la información sea aún mayor en el futuro.

La digitalización de los procesos industriales incorpora grandes oportunidades, quizás algunas muy necesarias para la humanidad. Seguramente las tecnologías y la digitalización de los sectores industriales ayudarán, entre otras cosas, a la reducción de las emisiones de CO2.

Frente a estas oportunidades que nos brindan las tecnologías disponibles, tales como c*loud, big data, machine learning, inteligencia artificial, IoT, 5G*, etc., se encuentran también las amenazas a las que dichas tecnologías están sometidas.

Hasta hace poco tiempo, en el entorno Industrial se tenía una falsa sensación de seguridad debido a la creencia de no existencia de riesgo. Esa sensación estaba basada principalmente en cinco ideas preconcebidas:

- La planta está aislada, no está conectada a internet.
- Tenemos un *firewall* que nos protege.
- Los hackers no saben de sistemas/procesos industriales.
- Mi planta no es objetivo de nadie.
- Los sistemas de *safety* de planta nos protegen de los ciberataques.

El riesgo que se debe gestionar está asociado a la probabilidad de que nuestros activos sufran una indisponibilidad o pérdida de integridad para prestar servicio o daños (impacto).

La visibilidad o superficie de exposición, que en las redes de entornos industriales, en adelante ***OT (Operation Technology)***, se ha visto incrementada en los últimos años y que por tanto, aumenta la probabilidad de un incidente de ciberseguridad.

En la actualidad, los sistemas *OT* padecen de los mismos males tradicionales que los sistemas ***IT (Information Technology)*** debido a la convergencia y la conectividad que estamos viviendo.

Las consecuencias de un mundo convergente, donde cada vez crece más la necesidad de mantener todo conectado, hacen que las redes industriales, históricamente aisladas, comiencen a tener la necesidad de conectarse, utilizando protocolos como *TCP/IP*, inseguros en su definición, encapsulando paquetes tradicionales de protocolos propietarios, como *MODBUS*.

Aunque una organización decida mantener el sistema *OT* desconectado de sus redes corporativas o de internet, los dispositivos que se utilizan para configurar y mantener estos, son portátiles, *pendrives*, tabletas y *smartphones*, que han tenido contacto previo con internet,

y con sistemas operativos *Microsoft Windows*, por lo que sigue existiendo riesgo si no se aplican políticas de seguridad.

Los sistemas de automatización y control industrial o ***ICS (Industrial Control Systems)***, y los sistemas ***SCADA (Supervisor Control and Data Acquisition)***, ampliamente conocidos estos últimos en el sector, estaban aislados de la red pública internet, incluso de la *LAN* privada de la organización. Disponían de sus propias redes *OT*, pero, poco a poco, sus protocolos propietarios y cerrados, convergieron hacia protocolos de red abiertos, buscando en ocasiones una reducción de costes en la programación y la gestión, que se decide hacer de forma remota aprovechando la infraestructura *IT* existente.

A nadie se le escapa el que existan instalaciones industriales, soportadas actualmente por sistemas operativos o *hardware*, cuyos fabricantes dejaron de dar soporte hace varios años o cuya incorporación de perfiles de ciberseguridad y por ende, cultura de ciberseguridad en los entornos industriales, es aún incipiente.

Seamos o no conscientes de lo que implica el párrafo anterior, el problema introducido es mayor de lo que parece, debido a que estamos juntando dos entornos *IT* y *OT*, con **necesidades de conocimiento específico y ciclos de vida diferentes**, que complicarán el establecimiento de **prioridades**, a la hora de disminuir el riesgo de ciberataque en la organización.

Se debe tener en cuenta también, que un incidente de ciberseguridad en un entorno industrial, puede tener **un impacto más allá del mundo digital**, donde un ciberataque *IT* tradicional podrá disminuir el valor de la organización, dañar su imagen de marca, etc., un entorno industrial es capaz de poner en marcha de forma automática actuadores y mecanismos que **modifican nuestro mundo físico** pudiendo provocar:

- Daños medioambientales.
- Afectación a la salud pública y a las vidas humanas.
- Interrupción de servicios esenciales para la ciudadanía.

Nos enfrentamos pues a grandes retos debido a la convergencia, la adopción de las *IT* en las *OT*, y la fuerte demanda de conectividad, donde han salido a la luz debilidades tradicionales en los sistemas *IT*, ahora en instalaciones críticas, y en ocasiones sin tener en cuenta que:

- En muchas ocasiones, el personal de planta o terceras personas, que hacen uso de estas tecnologías, no están **debidamente formados**.
- Derivado de lo anterior, se **desconocen los riesgos** que supone la utilización de ciertas tecnologías *IT* sobre entornos *OT*, no aplicando medidas de control.
- También sucede, que el personal de *IT*, *OT* y ciberseguridad no aúnan esfuerzos y conocimientos para aplicar medidas y controles de seguridad.

El caso más sonado, sin duda, ha sido ***Stuxnet***, pero cada vez son más las infraestructuras críticas que sufren alguna intrusión: plantas de energía, gas, metalúrgicas, *PLC* aislados en internet y un largo etcétera. Basta hacer una búsqueda en **shodan.io** o visitar su apartado dedicado a *ICS* para ver el número de equipos conectados a internet sin ningún tipo de salvaguarda. Igualmente, una consulta a la *MITRE ATT&CK for ICS*[1] permite valorar la cantidad de amenazas a las que estos sistemas están expuestas.

La automatización industrial no es algo novedoso, los *ICS* existen desde hace mucho tiempo y funcionan correctamente, sin embargo, la integración con las redes *TCP/IP* les hacen ser foco de atención, y ya no se les puede considerar entornos aislados. Organizaciones crimi-

[1] https://collaborate.mitre.org/attackics/index.php/Main_Page

nales o grupos patrocinados por estados, tienen capacidades y conocimiento para acceder a los controles de un sistema industrial/instalación por la vía del *malware* especializado y otras técnicas.

Por todo esto, aquellos que tienen la responsabilidad de brindar servicios esenciales, mantener negocios sostenibles, asegurar con éxito el desarrollo de la I+D nacional, o quienes tienen la responsabilidad de velar por la seguridad de la ciudadanía, tienen el gran desafío de hacerlo acompañando a los negocios de forma que sean competitivos, pero bajo unos niveles de riesgo conocidos, aceptados y gestionables.

Afortunadamente, la preocupación está, y en mayor o menor medida, todos los *stakeholders* (empresas del sector industrial, proveedores de servicios, universidades, reguladores, asociaciones) tienen planes para hacer frente a estos nuevos desafíos.

1.2 *Safety & Security*.

Sin lugar a duda, quienes diseñaron o diseñan instalaciones industriales, han tenido siempre muy en cuenta los aspectos de *safety*, pero quizás en el pasado no tuvieron en cuenta los aspectos de *security*, especialmente los de *cybersecurity*. El lenguaje español no distingue las acepciones de las palabras *SAFETY* y *SECURITY*, en inglés. Pero estas palabras sí que tienen conceptos diferenciales. De una forma muy resumida podría decirse:

"***Safety***" suele aplicarse a la protección contra riesgos más o menos fortuitos, tales como accidentales, desastres naturales, etc.

"***Security***" suele aplicarse a la seguridad ante actos de naturaleza intencionada (robos, intrusiones, vandalismo, agresiones. La ciberseguridad (*cybersecurity*) está dentro de este concepto, pero circunscrito al contexto de la seguridad de la información y los sistemas.

Cabe destacar que la ciberseguridad en el mundo *OT* no puede basarse en los mismos criterios y enfoques que se utilizan para el mundo *IT*. Por resumirlo se podría decir que en el mundo *IT* la ciberseguridad está gestionada con la información como punto central (***Information Centric***), mientras que en el mundo *OT* la ciberseguridad debe focalizarse con los procesos como punto central (***Process Centric***). De esta forma se consigue un mejor entendimiento entre los ingenieros de plantas y los expertos de ciberseguridad, tema que se hace fundamental en proyectos de mejora de la ciberseguridad industrial.

1.3 Redes de tecnologías de la operación (*OT) y* sistemas de control industrial (*ICS)*.

Los *ICS* se basan en 3 etapas:

- Medición de los datos del proceso (monitorización).
- Evaluación de la información obtenida en cuanto a parámetros estándar.
- Control del proceso en base a la información medida y evaluada.

Estos sistemas de control pueden ser completamente manuales, automatizados en su totalidad, o ambas formas (híbridos).

Los sistemas conocidos como *SCADA* permiten evaluar desde una consola la información de múltiples puntos de un proceso y tomar decisiones de control.

Esto nos lleva a la necesidad describir cuáles son los componentes habituales de una red *OT*:

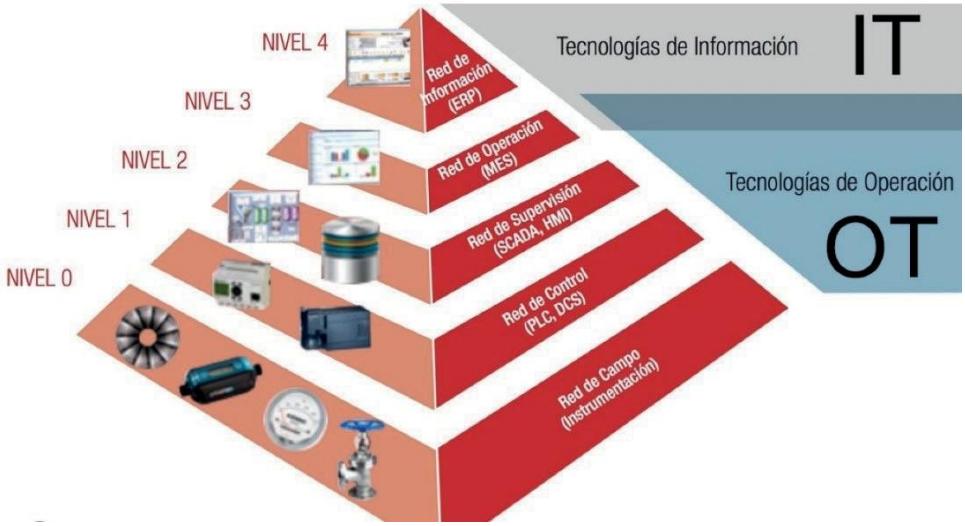


Ilustración1 https://www.cci-es.org/Guia_Piramide

Capa inferior (0). Capa de los Sensores y Actuadores, sería como la capa física, donde lo que importa es el medio o los dispositivos de campo y se transmiten señales, que pueden ser tanto analógicas como digitales, con las particularidades que ello implica.

Entrarían aquí, por ejemplo: sensores de movimiento, sensores de temperatura, sensores de niveles, sensores magnéticos, actuadores, etc.

Capa (1). Se puede encontrar:

- ***PLC*** (*Programmable Logic Controller)*, dispositivo que permite la automatización de un proceso electromecánico, controlando el funcionamiento de las máquinas empleadas en la producción.

- ***RTU*** (*Remote Terminal Unit*) un microprocesador capaz de adquirir señales de campo y actuar en consecuencia en base a una programación existente.

- ***DCS***[2] (*Distributed Control System*), se comunica con los dispositivos de campo y presenta los datos a un ***HMI*** (*Human-Machine Interface*), obteniendo información de los *PLC* o de las *RTU*.

Capa (2). Nivel de los ***HMI/SCADA***, que recolecta toda la información de los *PLC* y/o *RTU* distribuidos de manera automática, y empezamos a encontrarnos con un protocolo conocido: *TCP/IP*. Es el interfaz que utilizan, por ejemplo, los operadores de planta.

Capa (3). Nivel de los ***MES*** (*Manufacturing Execution System*) cuyo objetivo no es la evaluación del proceso en sí mismo, sino la de su eficiencia a partir de la información recibida.

Capa (4). Aquí tendrían cabida los ***ERP*** (*Enterprise Resource Planning*), donde básicamente se decide qué tipo de controles se ejecutarán, con qué frecuencia y con qué esfuerzo, con el objetivo de disponer de una planificación coherente.

[2] Los términos y conceptos de DCS y SCADA son muy similares entre sí, y en ocasiones se utilizan indistintamente, dependiendo del sector.

1.4 Seguridad en la cadena de suministro.

Las infraestructuras *OT* están muy vinculadas a servicios y tecnologías muy específicas, que necesitan ser provistos por especialistas, que en la mayoría de las veces son terceras partes y para ello requieren con frecuencia un importante nivel de interconexión con ellas. Asimismo, muchas de las organizaciones que proveen este tipo de servicios y que provienen del ámbito industrial, no poseen una cultura de ciberseguridad, ni cuentan en muchos casos con áreas expertas en esta materia. Esto implica que los sistemas del cliente sean accedidos por personal externo, expertos en los servicios que proveen, pero pertenecientes a organizaciones donde la seguridad está mucho menos desarrollada que en aquellas provenientes del campo de *IT*. Esto puede traer como consecuencia, prácticas inseguras que pongan en riesgo la infraestructura *OT*, ya de por sí más vulnerable por los puntos vistos anteriormente.

A través de los proveedores se pueden materializar infinidad de riesgos, siendo algunos de los más destacables, la explotación de vulnerabilidades de sistemas *OT* al exponerse a los equipos o redes de los proveedores, la infección de *malware* existente en los equipos o redes del proveedor, la exfiltración de información, al existir, en general, un bajo control de datos y tráfico intercambiado, la indisponibilidad de sistemas debido a acciones del proveedor que podría suponer un enorme impacto por la frecuente ausencia de copias de seguridad en estos entornos, etc. En general, los mismos riesgos que en el entorno *IT* pero agravados por la propia naturaleza de los entornos *OT* que se ha visto antes.

1.5 *IoT* & Privacidad.

Cabe destacar, que muchas redes *OT* en la actualidad están gestionando procesos industriales, pero los procesos de digitalización de la industria, con la incursión de soluciones *IoT* en entornos industriales, hace necesario que se tengan en cuenta aspectos relacionados con la privacidad, cuyo ámbito está fuertemente regulado por *GDPR*.

En este nuevo escenario de los entornos industriales que se fundamentan en la interconexión de múltiples dispositivos inteligentes que automatizan procesos y generan gran cantidad de información, plantean nuevas oportunidades que exigen una revisión del concepto de privacidad que se tenía tradicionalmente en los entornos industriales.

La recolección de datos personales de los usuarios es inherente al funcionamiento de estos dispositivos, con independencia del nivel de consciencia del empresario, profesionales técnicos y usuario en cuanto a la información personal que está revelando con el uso de este nuevo paradigma digital integrado en los entornos industriales.

Todo lo anteriormente expuesto, obliga a quienes estén inmersos en este tipo de proyectos a que deben realizar un análisis pormenorizado de los diferentes riesgos y amenazas a tener en cuenta en sus sistemas de operación, y de los diferentes tratamientos de datos personales que se puedan efectuar con los datos almacenados.

Por tanto, habrá que contemplar controles orientados a preservar la privacidad en los entornos industriales, donde la aplicación de los principios rectores de la normativa de protección de datos aplicable en Europa, como la privacidad por defecto y por diseño (*PbD*) es la mejor evidencia para demostrar la debida diligencia en el ejercicio de "responsabilidad proactiva" exigida en la misma.

Incluyendo los conceptos de *PbD*, se incorporan los principios de privacidad dentro de los procesos de diseño, operación y gestión de los sistemas de una organización para alcanzar un marco de protección integral en lo que a protección de datos se refiere.

Durante el desarrollo de la guía se verán distintos controles específicos para garantizar la privacidad de los datos de carácter personal que puedan almacenarse y tratar en los entornos industriales.

2. MARCO REGULATORIO

La Estrategia de Ciberseguridad Nacional.

La Orden PCI/487/2019, de 26 de abril, es la norma a través de la cual se publica la Estrategia Nacional de Ciberseguridad (en adelante, ENCS).

La ENCS es el marco de referencia de un modelo integrado cuyas bases son la implicación, coordinación y armonización de todos los actores y recursos del Estado, la colaboración público-privada, y la participación de la ciudadanía.

La Estrategia, para el logro de sus objetivos, crea una estructura orgánica, integrada en el marco del Sistema de Seguridad Nacional, que debe servir para articular la acción única del Estado conforme a unos principios compartidos por los actores en un marco institucional adecuado.

Los objetivos para la ciberseguridad, bajo los principios unidad de acción, anticipación, eficiencia y resiliencia por los que se rige la Estrategia, dedican un objetivo específico (Objetivo I) a la "Seguridad y resiliencia de las redes y los sistemas de información y comunicaciones del sector público y de los servicios esenciales".

En dicho objetivo se destaca la necesidad de que estos operadores se involucren activamente en un proceso de mejora continua respecto de la protección de sus sistemas, y se conviertan en modelo de buenas prácticas en la gestión de la ciberseguridad.

Además, se recoge el principio de responsabilidad compartida, en virtud del cual el sector público debe mantener estrechas relaciones con las empresas estratégicas e intercambiar conocimiento para garantizar la adecuada coordinación y cooperación en el entorno de la ciberseguridad.

La Estrategia desarrolla, por último, el marco estratégico e institucional compuesto por los *CSIRT* de referencia o equipos de respuesta a incidentes que analizan los riesgos y que, como puerta de entrada, supervisan los incidentes, difunden alertas y aportan soluciones para mitigar sus efectos, remitiendo las notificaciones oportunas a las Autoridades competentes.

Ley de Protección de las Infraestructuras Críticas

La Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas ("Ley PIC"), traspone la Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección.

Por infraestructura crítica se entiende aquel elemento, sistema o parte de este cuyo funcionamiento resulta indispensable para el mantenimiento de las funciones sociales vitales, la salud, la integridad física, la seguridad y el bienestar social y económico, y cuya perturbación o destrucción tendría graves consecuencias.

La Ley concibe la seguridad al servicio del ciudadano y del Estado, estableciendo objetivos y líneas de acción para la protección de infraestructuras críticas, y tiene por objeto "establecer las estrategias y las estructuras adecuadas que permitan dirigir y coordinar las actuaciones de los distintos órganos de las Administraciones Públicas en materia de protección de infraestructuras críticas, previa identificación y designación de las mismas, para mejorar la prevención, preparación y respuesta de nuestro Estado frente a atentados terroristas u otras

amenazas que afecten a infraestructuras críticas. Para ello se impulsará, además, la colaboración e implicación de los organismos gestores y propietarios de dichas infraestructuras, a fin de optimizar el grado de protección de estas contra ataques deliberados de todo tipo, con el fin de contribuir a la protección de la población".

Derivado de la Ley y de su Reglamento de desarrollo, en 2012 se constituyó el Sistema Nacional de Protección de Infraestructuras Críticas (Sistema PIC) que consiste en un conjunto de agentes del sector público y privado con competencias y responsabilidades en esta materia.

La Ley PIC aporta, asimismo, la creación del Catálogo Nacional de Infraestructuras Estratégicas como instrumento con toda la información y valoración de las infraestructuras estratégicas, y crea el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), que es el órgano encargado del impulso, coordinación y supervisión de las actividades encomendadas al Ministerio del Interior en relación con la protección de infraestructuras críticas en España.

Por último, de la Ley PIC emana el Plan Nacional de Protección de Infraestructuras Críticas, con el fin de dirigir y coordinar las actuaciones para proteger las infraestructuras críticas, y los Planes Estratégicos Sectoriales, que recogen los criterios definidores de las medidas a adoptar para hacer frente a una situación de riesgo partiendo de las características propias de cada uno de los sectores.

Reglamento de protección de las infraestructuras críticas

La Ley PIC se desarrolla a través del Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

Su finalidad es la de desarrollar, concretar y ampliar los aspectos contemplados en la citada Ley, teniendo en cuenta la necesaria articulación de los órganos y entidades, tanto de las Administraciones Públicas como del sector privado, así como el diseño de un planeamiento orientado a la prevención y protección de las infraestructuras críticas frente a las amenazas o actos terroristas que eventualmente puedan utilizar como canal a las tecnologías de la información y las comunicaciones.

El Reglamento prevé que los operadores de infraestructuras críticas designen a un Responsable de Seguridad y Enlace, así como un Delegado de Seguridad por cada una de las infraestructuras críticas identificadas, que tendrán las competencias recogidas en la propia norma.

El Reglamento contempla los Planes de Seguridad del Operador, como documentos estratégicos definidores de las políticas para garantizar la seguridad del conjunto de instalaciones o sistemas de su propiedad o gestión. Asimismo, se prevén los Planes de Protección Específicos, como documentos operativos donde se deben definir las medidas adoptadas y las que se vayan a adoptar por los operadores para garantizar la seguridad integral, ya sea física o lógica, de las infraestructuras de su propiedad o gestión.

Sus artículos 23 y 26 (Aprobación, registro y clasificación) prevén la aprobación de los Planes de Seguridad del Operador y Planes de Protección Específicos o las propuestas de mejora de los mismos, para lo que se promueve el desarrollo de un esquema de acreditación que podrá estar basado en un estándar internacional (*NIST, ISO/IEC*), o en una normativa específica (en el caso de España, el Esquema Nacional de Seguridad aprobado mediante el Real Decreto 3/2010, de 8 de enero).

Esquema Nacional de Seguridad

El Real Decreto 3/2010, de 8 de enero, regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (en adelante ENS).

El ENS tiene por objeto "establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada".

El ámbito de aplicación del ENS es el Sector Público, que se compone por las instituciones cuyo funcionamiento se rige por los artículos 2º de las leyes 39/2015 y 40/2015, respectivamente, y lo indicado sobre el sector público institucional.

El mandato principal del ENS viene establecido en su artículo 11, según el cual "todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad que articule la gestión continuada de la seguridad, que será aprobada por el titular del órgano superior correspondiente". Esta política de seguridad se establecerá en base a unos principios básicos y se desarrollará aplicando los requisitos mínimos previstos en el propio Esquema.

Desde su aprobación, el ENS ha sido, primero modificado por el Real Decreto 951/2015, al objeto de actualizarlo a las nuevas necesidades tecnológicas, así como al contexto regulatorio internacional y europeo.

Posteriormente, por la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, que en su apartado VII (Soluciones y servicios prestados por el sector privado) indica: "Cuando los operadores del sector privado presten servicios o provean soluciones a las entidades públicas, a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categoría BÁSICA, o la Certificación de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categorías MEDIA o ALTA, utilizando los mismos procedimientos que los exigidos en esta Instrucción Técnica de Seguridad para las entidades públicas.".

Esta última referencia normativa va alineada con lo dispuesto en la Disposición Adicional primera de la Ley Orgánica de Protección de datos y garantía de derechos digitales, Ley 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Ley de seguridad de las redes y sistemas de información

Mediante el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, se transpuso al ordenamiento jurídico español la Directiva europea 2016/1148 (conocida como Directiva *NIS*) relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión Europea.

El Real Decreto-ley tiene por objeto regular la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y de los servicios digitales, y establecer un sistema de notificación de incidentes en nuestro país.

Dicha norma determina, asimismo, la forma y criterios de identificación de los servicios esenciales y de los operadores que los presten. Además, recoge el marco estratégico e insti-

tucional de la seguridad de las redes y sistemas de información en España haciendo énfasis en la cooperación entre autoridades públicas.

También se disponen las potestades de inspección y control de las autoridades competentes y la cooperación con las autoridades nacionales de otros Estados miembros, se tipifican una serie de infracciones y sanciones, y se establecen las obligaciones de seguridad de los operadores.

Finalmente regula la notificación de incidentes, con especial atención a los incidentes con impacto transfronterizo y a la información y coordinación con otros Estados de la Unión Europea para su gestión.

Desarrollo de la Ley de seguridad de las redes y sistemas de información

El Real Decreto-ley 12/2018 ha sido desarrollada a través del Real Decreto 43/2021, de 26 de enero, que transpone de manera definitiva la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

En este Real Decreto se desarrollan cuestiones como la figura del Responsable de Seguridad de la Información, se establecen las medidas de seguridad mínimas que se han de adoptar, relaciona las Autoridades sectoriales competentes, establece una plataforma única de notificación de incidentes y relaciona los incidentes que han de ser comunicados, entre otras cuestiones.

ISA 99/IEC62443, ISO 27001, ISO 27002, NIST 800-82

Existen diferentes estándares internacionales que abordan de alguna manera la ciberseguridad de los sistemas industriales.

Entre otros, cabe destacar el estándar *ISA 99/IEC62443* que constituye un marco de referencia internacional para la ciberseguridad de sistemas *OT*.

Este estándar pone el foco en la disponibilidad y la integridad de los elementos más importantes, estableciendo un ciclo de vida para la ciberseguridad industrial consistente en tres pasos: evaluación, desarrollo e implementación y mantenimiento.

Podemos considerar además otros estándares como las *ISO 27001 y 27002* en cuanto a la seguridad de la información, o la *SP NIST 800-82*, que aborda la seguridad en los sistemas de control industrial, proporcionando una visión general de los *ICS* y las topologías típicas de los sistemas, identificando amenazas y vulnerabilidades, así como las correspondientes contramedidas de seguridad.

3. RECOMENDACIÓN DE MEDIDAS BÁSICAS DE SEGURIDAD

Antes de comenzar a desarrollar el presente capítulo, es muy importante señalar que tanto el Real Decreto-ley de seguridad de las redes y sistemas de información, como la LPIC o el ENS, establecen como punto de partida para la elección de las salvaguardas el análisis de riesgos.

Alineados con ese pilar básico, el objetivo de este apartado es sugerir un marco de medidas a modo de guía orientativa para los Operadores de servicios Esenciales (OSE) que presten servicios basados en infraestructura *OT*, de forma que permita disponer de mecanismos de prevención, detección, respuesta y recuperación ante incidentes de ciberseguridad en los sistemas de control industrial del operador. Dicho marco de medidas aportará información relevante para el análisis de riesgo, ayudando a verificar que los controles seleccionados cubren al menos el conjunto de medidas que identificamos en este capítulo. Finalmente, pretende minimizar los impactos que pueden afectar a la operación de las instalaciones, evitando pérdidas económicas, daños físicos, medioambientales y reputacionales.

3.1 Gestión de la ciberseguridad en Sistemas de Control Industrial (SCI).

La ciberseguridad de los SCI de los OSE se podrá gestionar mediante procesos globales y/o locales dependiendo del tamaño y tipo de operador.

Con el objetivo de establecer las prácticas con el mayor nivel de detalle posible de acuerdo a la realidad de cada entorno, se recomienda establecer o adaptar estas medidas en diferentes niveles operacionales, tomando como referencia los diferentes niveles del modelo de arquitectura *PERA* (por sus siglas en inglés, *Purdue Enterprise Reference Architecture*).

3.2 Medidas básicas recomendadas.

1- Asignación de roles y responsabilidades. Esta es una de las medidas más relevantes, no solo por su importancia, sino porque es la base para poder asegurar que las siguientes puedan implantarse y mantenerse, de forma que se cumplan con el objetivo marcado. En la medida de lo posible y basado en el modelo general de gobierno de compañía, debería asegurarse una segregación de funciones, de forma que se puedan identificar claramente las responsabilidades y las capacidades ejecutivas y técnicas que debe de tener cada rol.

- **Gobierno de la ciberseguridad en SCI**. Debe existir un rol de gobierno de la ciberseguridad en SCI y asignarse dentro de la estructura organizativa de la compañía.
- **Responsable de seguridad de la instalación**. Es el máximo responsable de la seguridad de la instalación.
- **Propietarios del SCI.** Es el responsable del sistema de control industrial.

2- Estrategia de Seguridad. Disponer de una estrategia de seguridad en las redes *OT* ayuda a garantizar el cumplimiento del resto de medidas indicadas a continuación. Esta estrategia debe estar formada, al menos por los siguientes puntos:

a. Marco normativo interno de seguridad integrando *IT* y *OT* (políticas, normas y procedimientos).

b. Necesidad de aplicar la gestión de riesgos para aplicar las medidas de seguridad adecuadas.

c. Necesidad de llevar a cabo la gestión de vulnerabilidades tecnológicas de los activos que constituyen las redes *OT*.

d. Gestión de incidentes de ciberseguridad.

3- Inventario actualizado de los SCI de la instalación. Disponer de un inventario completo de equipos SCI que se mantenga actualizado mediante la incorporación de los cambios resulta fundamental para la gestión de la seguridad en los SCI. Este inventario se puede utilizar en los análisis de riesgos y vulnerabilidades, así como en la respuesta ante incidentes. Los diferentes SCI de cada instalación deben de ser clasificados según criticidad para la prestación del servicio. Siendo esta la base del documento de aplicabilidad de los sistemas para la instalación.

En relación con el inventario, disponer de una guía de bastionado de los SCI actualizada en la que se recojan las buenas prácticas de configuración. Este guía recogerá las configuraciones generales de todos los SCI clasificadas por fabricante y será mantenida por los propietarios de los activos con el apoyo de los custodios.

4- Control de acceso lógico de los SCI. Disponer de medidas de control de acceso lógico a los SCI garantiza que una determinada entidad, usuario o proceso pueda, o no, acceder a un recurso del sistema para realizar una determinada acción. Para garantizar que los SCI cuentan con medidas de control de acceso adecuadas se debe tener en cuenta:

a. Que todo acceso esté prohibido, salvo concesión expresa.

b. Que la entidad quede identificada singularmente.

c. Que la utilización de los recursos esté protegida.

d. Que se definan para cada entidad los siguientes parámetros: a qué se necesita acceder, con qué derechos y bajo qué autorización.

e. Serán diferentes las personas que autorizan, usan y controlan el uso.

f. Que la identidad de la entidad quede suficientemente autenticada.

g. Que se controle tanto el acceso local como el acceso remoto (ver apartado “Control y supervisión de acceso remoto” incluido posteriormente).

5- Se configurarán los equipos SCI previamente a su entrada en operación, de forma que:

a. Se retiren cuentas y contraseñas estándar.

b. Se aplique la regla de "mínima funcionalidad":

1. El sistema debe proporcionar la funcionalidad requerida para que la organización alcance sus objetivos y ninguna otra funcionalidad.

2. El sistema no proporcionará funciones de operación, ni de administración, ni de auditoría, reduciendo de esta forma su perímetro al mínimo imprescindible.

3. Se debe desactivar mediante el control de la configuración, aquellas funciones que no sean de interés, no sean necesarias, e incluso aquellas que sean inadecuadas al fin que se persigue.

c. Se aplique la regla de "seguridad por defecto".

6- Arquitectura de Seguridad de redes *OT*. La seguridad de los SCI debe ser objeto de un planteamiento integral detallando, al menos, los siguientes aspectos:

a. Documentación de las instalaciones:

1. Áreas.

2. Puntos de acceso.

b. Documentación del sistema:

1. Equipos.

2. Redes internas y conexiones al exterior.

3. Puntos de acceso al sistema (puestos de trabajo y consolas de administración).

c. Esquema de líneas de defensa:

1. Puntos de interconexión a otros sistemas o a otras redes.

2. Cortafuegos y *DMZ*.

3. Utilización de tecnologías diferentes para prevenir vulnerabilidades que pudieran perforar simultáneamente varias líneas de defensa.

7- Segregación entre las redes de control y corporativas. La segregación entre la red del SCI y la corporativa garantiza una comunicación controlada y segura entre ambas, lo que proporciona protección recíproca frente a ataques cibernéticos provenientes de la otra red.

Desde el punto de vista de seguridad, se puede ver cada una de las distintas subredes como zonas con distintos requisitos de seguridad. La seguridad se consigue restringiendo los flujos de información entre esas zonas mediante soluciones de *SW* o *HW*. De esta manera se evita la propagación de ataques entre dichas subredes. Como ejemplo, las normas *IEC-62443-1-1 e IEC-62443-3-3* proporcionan definiciones y medidas de seguridad para las zonas y conductos; o la norma *IEC-62351*, que aborda medidas de seguridad para sistemas de control aplicados a entornos de energía, muchas de las cuales se pueden generalizar para cualquier sistema industrial.

La segmentación entre la red del SCI y la corporativa se debe segmentar garantizando que haya:

a. Control de entrada de los usuarios que llegan a cada segmento.

b. Control de salida de la información disponible en cada segmento.

c. Las redes se pueden segmentar por dispositivos físicos o lógicos. El punto de interconexión estará particularmente asegurado, mantenido y monitorizado.

8- Trazabilidad. Se deben registrar las actividades de los usuarios en los sistemas SCI, de forma que:

a. El registro indique quién realiza la actividad, cuándo la realiza y sobre qué información.

b. El registro incluya la actividad de los usuarios y, especialmente, la de los operadores *OT* y administradores en cuanto puedan acceder a la configuración y actuar en el mantenimiento del sistema.

c. El registro de las actividades realizadas con éxito y los intentos fracasados.

9- Gestión de incidentes. Se debe disponer de un procedimiento de gestión de incidentes de seguridad que garantice la adecuada gestión de mismo. Este procedimiento debe garantizar el tratamiento de incidentes de seguridad que puedan tener un impacto en la seguridad de los SCI, incluyendo:

a. Procedimiento de reporte de incidentes reales o sospechosos, detallando el escalado de la notificación.

b. Procedimiento de toma de medidas urgentes, incluyendo la detención de servicios, el aislamiento del sistema afectado, la recogida de evidencias y protección de los registros, según convenga al caso.

c. Procedimiento de asignación de recursos para investigar las causas, analizar las consecuencias y resolver el incidente.

d. Procedimientos para informar a las partes interesadas, internas y externas.

e. Procedimientos para:

1. Prevenir que se repita el incidente.

2. Incluir en los procedimientos de usuario la identificación y forma de tratar el incidente.

3. Actualizar, extender, mejorar u optimizar los procedimientos de resolución de incidentes.

10- Gestión de vulnerabilidades. Con el objetivo de prevenir los riesgos tecnológicos asociados a los SCI se debe llevar a cabo un plan de gestión de vulnerabilidades de estos, el cual debe de considerar los siguientes aspectos:

a. Contar con un mapa de activos actualizado de la red *OT*.

b. Contar con una herramienta automática de escaneo de vulnerabilidades.

c. Establecer escaneos periódicos de los activos de la red *OT* priorizando los activos críticos.

d. Subsanar las vulnerabilidades identificadas.

e. Creación de métricas e indicadores para potenciar el seguimiento de los resultados obtenidos.

11- Medidas *anti-malware* actualizadas. Las medidas destinadas a prevenir que los SCI puedan infectarse con *malware* y evitar su propagación, lo que garantiza la operación segura y fiable de los SCI. Estas medidas incluyen controles a nivel procedimental y técnico, destinados a detectar *malware* y prevenir infecciones. Asimismo, se debe contar con herramientas de detección o de prevención de intrusión (sondas análisis de tráfico).

12- Medidas preventivas y reactivas frente a ataques de denegación de servicio. Para ello se dotará a los SCI de estas medidas, para lo cual:

a. Se establecerá un sistema de detección de ataques de denegación de servicio.

b. Se establecerán procedimientos de reacción a los ataques, incluyendo la comunicación con el proveedor de comunicaciones.

c. Se impedirá el lanzamiento de ataques desde las propias instalaciones perjudicando a terceros.

13- Medidas de seguridad en relación con el uso de redes *WIFI* corporativas. En el caso en que los SCI hagan uso de redes *WIFI* corporativas, estas deberán contar con las siguientes medidas de seguridad:

a. Contar con un inventario de dispositivos haciendo una revisión periódica de este y de las posibles vulnerabilidades.

b. Crear una red de gestión exclusiva, que solo transporte tráfico de gestión y administración, en la que se empleen protocolos seguros.

c. Utilizar sistemas de autenticación centralizada como servidores *RADIUS* utilizando canales seguros.

d. Realizar una asignación mediante *DHCP* de dirección *IP* fija para cada cliente/dispositivo en cada una de las distintas redes.

e. Configurar los clientes para utilizar el protocolo *802.1X-EAP-TLS*, agente *NAC* y túnel *VPN* cifrado según lo recomendado.

f. Limitar el acceso físico a los equipos, así como el acceso lógico en función de los roles definidos y desactivar el servicio cuando no se esté utilizando.

g. Implementar sistemas de Detección de Intrusiones (*IDS*) para la detección de posibles anomalías que generen alarmas.

h. Monitorizar el tráfico de la red y realizar una búsqueda periódica de anomalías.

14- Procedimiento de parcheo para aplicaciones, sistemas operativos y *firmware*. Los parches de seguridad los publican los proveedores de sistemas operativos, *software* de aplicaciones y equipos para solucionar posibles vulnerabilidades en sus productos que pueden ser aprovechadas por atacantes potenciales. Los parches de seguridad deben ser aplicados según los procedimientos internos y siempre que estén validados por los fabricantes para la instalación en cuestión. Los contratos con proveedores de *software* deben contemplar los servicios parches de seguridad y la validación de los mismos en cada una de las instalaciones industriales.

15- Los equipos portátiles y dispositivos móviles que tengan acceso a redes *OT*, deberán cumplir con las siguientes medidas de seguridad:

a. Contar con un inventario de equipos portátiles junto con una identificación de la persona responsable del mismo y un control regular de que está positivamente bajo su control.

b. Establecer un canal de comunicación para informar, al servicio de gestión de incidentes, de pérdidas o sustracciones.

c. Limitar la información y los servicios accesibles a los mínimos imprescindibles, requiriendo autorización previa de los responsables del SCI y los servicios afectados.

d. Evitar en la medida de lo posible, que el equipo contenga claves de acceso remoto a la organización. Considerar claves de acceso remoto aquellas que sean capaces de habilitar un acceso a otros equipos de la organización, u otras de naturaleza análoga.

16- Protocolos seguros. Para garantizar la confidencialidad del tráfico generado por los SCI, estos deberán emplear protocolos considerados como seguros y soluciones específicas destinadas a tal efecto.

17- Controles para dispositivos extraíbles. Los medios extraíbles (ej.: memorias *USB*, discos duros externos, unidades *CD-ROM/DVD*) son una de las vías más habituales de infección por *malware*. Eliminar, o al menos, reducir el uso de medios extraíbles siempre que sea técnicamente posible y controlar su utilización cuando lo anterior no sea posible, reduce de manera notable el riesgo de infección por *malware*.

18- Control y supervisión de acceso remoto. Deberá implementarse mediante métodos seguros. El acceso remoto a los SCI presenta mecanismos potencialmente dañinos por *malware* y acceso no autorizado a los SCI, que pueden incidir en la operación segura y fiable. El acceso remoto ha de contar con una justificación de negocio e implementarse de forma que esté garantizada su seguridad y que únicamente personas autorizadas puedan hacer uso de esta funcionalidad.

Es recomendable que las comunicaciones de los dispositivos SCI con el exterior sean canalizadas a través de un *firewall*, que preferiblemente se defina una *DMZ* donde se alojen los servicios a los que se puedan conectar los dispositivos SCI y sean los servicios alojados en esta, los que se puedan conectar al exterior. De esta manera se limita mejor el perímetro y es más sencillo de proteger.

Asimismo, se aconseja implementar mecanismos que permitan limitar o bloquear los flujos de información para evitar la propagación de amenazas. En ese sentido, se recomienda bloquear cualquier protocolo de comunicación que no sea necesario para el teleservicio/acceso remoto, con el fin de reducir la superficie de ataque.

Finalmente, los accesos remotos a la infraestructura deben de ser monitorizados y registrados, de manera que puedan ser auditados en un futuro.

19- Plan de respuesta ante incidentes. Resulta esencial que los activos/instalaciones estén preparados ante tal eventualidad, a fin de minimizar su impacto y recuperar el nivel habitual de funcionamiento en el menor tiempo posible. Dada la imposibilidad de prever cada posible tipo de incidente, los planes se centran en la gestión del mismo, garantizando que el personal esté concienciado sobre la problemática de la ciberseguridad, formado para identificar fallos en planta como consecuencia de posibles fallos y/o sabotajes en los SCI. El personal se involucra activamente en el diseño, elaboración y pruebas de los ciberincidentes, estableciendo comunicaciones fluidas y la asignación clara de responsabilidades. Resulta fundamental ensayar los planes para someterlos a prueba y que todo el personal involucrado se familiarice con ellos.

20- Capacidades de copia de seguridad y restauración. La recuperación tras un incidente de seguridad, un fallo de *hardware* o *software* o un problema de corrupción de datos, pueden requerir la restauración total o parcial de uno o varios dispositivos o del sistema en su conjunto.

21- Control estricto sobre roles de administración y la Gestión del Cambio sobre los SCI. Los roles de administración, disponen de privilegios para realizar cambios en los SCI que pueden repercutir en la operación segura y fiable de los SCI, así como de la instalación controlada por estos. Los cambios en los SCI fuera de las operaciones rutinarias (ej.: cambio de *setpoints*, arranque/parada de equipos, apertura/cierre de válvulas) deben someterse a un estricto control, empleando los procesos de gestión del trabajo (ej.: permiso de trabajo) y gestión del cambio existentes en el activo o instalación, a fin de garantizar que los cambios se apliquen únicamente tras pasar por el proceso pertinente de diseño, revisión, pruebas y aprobación.

22- Gestión de archivos de registro y pistas de auditoria. Los archivos de registro y pistas de auditoría son necesarios tanto para la monitorización de eventos de seguridad y detección de anomalías como para la realización de análisis forenses tras cualquier incidente de seguridad.

23- Seguridad de la cadena de suministro. Para establecer un mecanismo seguro en la cadena de suministro, se relacionan las siguientes recomendaciones:

- Establecer un marco para gestionar el ciclo de vida del sistema de control industrial, centrándonos en seguridad por diseño, para minimizar las vulnerabilidades y así reducir la superficie de ataque (ver gestión de riesgos de ciberseguridad).

- Establecer alianzas duraderas en el ámbito de la ciberseguridad con todos los socios. Redactar contratos con acuerdos contractuales específicos sobre Ciberseguridad. Unificar políticas, normas y procedimientos.

- Elevar el nivel de formación y concienciación en ciberseguridad, tanto del personal interno *IT* y *OT*, como externo (proveedores, socios, etc), que estén involucrados en la operación de los sistemas de control industrial. Crear grupos de trabajo transversales *IT/OT* para que la cultura de ciberseguridad definida por la empresa se difunda en todos los niveles. Revisar periódicamente que el personal tiene el nivel requerido de competencia y habilidades (test, píldoras informativas, etc.).

- Análisis e intercambio de inteligencia sobre amenazas cibernéticas dentro del sector, como con los proveedores tecnológicos. Especial atención a los fabricantes de SCI. Establecer la obligatoriedad de notificación de vulnerabilidades, tan pronto se tenga conocimiento de ellas (diligencia especial dentro del mismo sector).

- Realizar revisiones periódicas de la estrategia de gestión de riesgos tecnológicos incluyendo a los socios de la cadena de suministro. Evaluación conjunta de vulnerabilidades, garantizando que el riesgo que surja de las deficiencias se aborda con una adecuada gestión de remediciónintegral.

- **Formación y concienciación del personal de** *OT***.** Se formará regularmente al personal técnico y de operación *OT* en aquellas materias que requieran para el desempeño de sus funciones, en particular en lo relativo a:

  a. Configuración de sistemas.

  b. Detección y reacción a incidentes.

  c. Gestión de la información en cualquier soporte en el que se encuentre. Se cubrirán al menos las siguientes actividades: almacenamiento, transferencia, copias, distribución y destrucción.

Se realizarán las acciones necesarias para concienciar regularmente al personal técnico y de operación *OT* acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos.

En particular, se recordará regularmente:

  a. La normativa de seguridad relativa al buen uso de los sistemas.

  b. La identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado.

  c. El procedimiento de reporte de incidentes de seguridad, sean reales o falsas alarmas.

- **Seguridad Física.** Las instalaciones donde se ubiquen los SCI dispondrán de elementos adecuados para el eficaz funcionamiento del equipamiento allí instalado. Y, en especial:

  a. Condiciones de temperatura y humedad.

  b. Protección del cableado frente a incidentes fortuitos o deliberados.

  c. Medidas de protección contra incendios.

  d. Medidas de protección contra inundaciones.

4. RESULTADOS OBTENIDOS

Las 116 carencias detectadas y las medidas compensatorias propuestas para su subsanación por las entidades colaboradoras se adjuntan en el **ANEXO I** del presente documento, agrupadas en 15 ámbitos para una mejor comprensión y facilidad de análisis.

Sobre este punto conviene incidir que muchas de las medidas recogidas en este Anexo I podrían ser también aplicadas a las subcontratas/proveedores.

Adicionalmente se incluye en el **ANEXO II** el estudio estadístico sobre las brechas de seguridad detectadas, así como el origen de la información.

En el **ANEXO III** se realiza una adaptación del catálogo de amenazas propuesto en la metodología MAGERIT, la cual está inicialmente destinada a sistemas de información. Este anexo proporciona algunos detalles que deben ser tenidos en cuenta en el tratamiento de redes en entornos *OT*.

Finalmente, en el **ANEXO IV** se incluye el glosario de términos.

ANEXO I – RESULTADOS DE LA CONSULTA

	ACCESOS LÓGICOS LOCALES	
	CARENCIA DE SEGURIDAD	**MEDIDAS COMPENSATORIAS**
1	Necesidad de permanencia de sesiones abierta en sistemas de supervisión impide la trazabilidad y auditoría.	Aumentar las medidas de control físico y a nivel de las redes. Sistema paralelo de registro de operador. Dispositivos adicionales en red que permitan establecer mecanismos de control de sesiones y bloqueo.
2	Control de sesiones y bloqueo en caso de ser necesario.	Aumentar las medidas de control físico y a nivel de las redes. Sistema paralelo de registro de operador. Dispositivos adicionales en red que permitan establecer mecanismos de control de sesiones y bloqueo. Integración de los intentos de sesión, tanto exitosos como fallidos, en *SIEM*.
3	Contraseñas "*hardcodeadas*". En muchos sistemas industriales existen contraseñas *hardcodeadas* de administración que, además, se encuentran publicadas en foros por internet.	Establecer controles a nivel de red sobre quién se conecta al equipamiento. Estos controles se pueden realizar con un *NGFW* industrial obligando al usuario, antes de conectarse al equipo afectado, a realizar una primera validación contra el *FW* y securizando la conexión entre el *FW* y el dispositivo fina en el caso de que el *FW* esté dotado de esta tecnología.
4	Existencia de un único usuario para todos los operadores. Permisos de administración para todos los usuarios. Política de contraseña débil, inexistente o la imposibilidad del software *OT* de adecuarse a una política de contraseñas robusta.	Creación de una política de credenciales y administración de usuarios que incluya, al menos: Creación de usuarios personalizados. Perfilado *RBAC (Role Based AccessControl)*. Políticas de contraseñas robustas. Registrar e identificar a las personas que hagan uso del usuario genérico compartido en caso de que no se pueda definir uno específico. Habilitar los *logs* de acceso y actividad en los sistemas a gestionar. Asegurar una identificación horaria de los usuarios que han accedido a la consola de operación. Puede ser con identificación con huella, con videovigilancia de la sala de operación, consola central de control de cuentas.

ANEXO I – RESULTADOS DE LA CONSULTA

5	Ciclo de vida de los usuarios	Implantación de políticas de gestión de privilegios asociada al ciclo de vida de los usuarios (p.e. asignación y revocación de accesos).
6	Usuarios con privilegios elevados con accesos a los sistemas.	Creación de cuentas nominales con los mínimos permisos funcionales.
7	Uso compartido de las cuentas locales administradoras.	Monitorización del uso de las cuentas compartidas mediante un registro independiente de entrada y salida al sistema.
8	Contraseñas embebidas en texto plano para aplicaciones.	Rotado de contraseñas embebidas en aplicaciones para evitar el conocimiento de las mismas.
9	Ausencia de doble factor de autenticación.	Integración de dobles factores de autenticación para el acceso a los sistemas.
10	Ausencia de flujos de trabajo de aprobación para cuentas críticas.	Creación de flujos de aprobación para cuentas con criticidad.
11	Ausencia de sistemas de monitorización y control de accesos.	Integración de sistemas de auditoria para el control de cuentas y accesos. Grabación de sesiones.
12	Ausencia sobre el control de políticas de contraseñas.	Integración de políticas de rotado eficientes, controladas y supervisadas de contraseñas.
13	Falta de control de las altas de usuarios en la consola de operación.	Implantar un proceso de autorización con segregación de funciones.
14	Federación segura en determinados escenarios *OT* como puede ser los sistemas de *Smart Grids*, en el que es necesario aplicar procedimientos de autenticación y de autorización estandarizados y siguiendo modelos distribuidos o descentralizados.	Estandarización de entornos federados *OT*, y siguiendo modelos de autenticación y autorización estandarizados, como por ejemplo el *RBAC* (IEC-62351-8), y bajo construcciones de red siguiendo los modelos de interconexión estándar. Estos puntos de interconexión normalmente deben/pueden recaer en g*ateways*, *proxies* o servidores de *Cloud*, *Fog o Edge*.

ANEXO I – RESULTADOS DE LA CONSULTA

	ACCESOS REMOTOS (USUARIO, MANTENIMIENTO, ETC.)	
	CARENCIA DE SEGURIDAD	**MEDIDAS COMPENSATORIAS**
1	Tele mantenimientos inseguros	Utilización de *VPN*. Creación de políticas de mantenimiento. Registro de todas las acciones de administración y mantenimiento llevadas a cabo de forma remota. Se puede reforzar mediante el empleo de un servidor de salto virtualizado que permita grabar entradas de teclado y las propias sesiones. Mención especial a los *softwares* de acceso remoto.
2	Interconexión del *OT* a la nube en la externalización de servicios.	Evaluar la posibilidad de centralizar la información en un único punto de gestión para la parte *OT* e *IT/Cloud*, simplificando las labores de los administradores de seguridad.
3	Uso de dispositivos móviles en el mundo *OT*.	Proteger estos nuevos mecanismos de conectividad con una solución de control de acceso que se pueda instalar en la línea de producción. Es deseable, para evitar introducir distintos elementos en la línea, que la solución cuente con la capacidad de facilitar el acceso a la red móvil. En el caso de dispositivos móviles corporativos, debe procederse al enrolamiento de los mismos en soluciones *MDM*. Definición de una lista blanca de dispositivos y/o implementación de soluciones que permitan llevar a cabo control o restricciones de los dispositivos móviles que accedan a la red *OT*.
4	Excesiva delegación a terceros en labores de mantenimiento.	Renegociación de contratos más favorable al cliente y con un control más exhaustivo sobre los contratos.
5	Accesos remotos a planta (parte *OT*) descontrolados o no auditables, por parte de terceras personas o subcontratas de partes de las instalaciones.	Gestión de accesos remotos seguros a planta y desde un único punto centralizado pasando por ambos *NGFW* que realizan la segregación *IT/OT*.
6	Gestión/administración de los sistemas industriales desde *PC* con salida a internet.	*Whitelisting* de equipos que permiten tener acceso a los sistemas *OT*.

ANEXO I – RESULTADOS DE LA CONSULTA

	PROTECCIÓN FRENTE A ATAQUES	
	CARENCIA DE SEGURIDAD	**MEDIDAS COMPENSATORIAS**
1	Inexistencia de seguridad proactiva. No existen mecanismos de seguridad proactiva en las redes industriales. Falta de sistemas de detección de ataques avanzados.	Contar con sistemas de protección reactiva como cortafuegos, sistemas *IPS*, sistemas de análisis de comportamiento, etc. Los cuales bloqueen los intentos de explotación de las vulnerabilidades de los sistemas industriales. Estos sistemas deben de contar también con capacidades antivirus, *Antibot*, control de ficheros y al menos *IPS* para la realización de *Virtual Patching* de las vulnerabilidades conocidas. Establecer procesos formales y herramientas a de Gestión de software malicioso / antivirus. Incluir funcionalidades *EDR* para la monitorización del comportamiento en los dispositivos que lo permitan.
2	Ataques de Denegación de Servicio.	Implementación de capacidades de detección de ataques *DOS* y *DDOS*. Implementación de capacidades de bloqueo y/o limitación del origen del ataque. Definición de planes de continuidad de negocio y minimización de riesgos asociados.
3	Protección ante ataques complejos.	Progresar en los sistemas de detección de intrusiones basados en anomalías (y, por tanto, en IA y *machine-learning*), e investigar en detección distribuida con soporte en técnicas de aprendizaje automático, *Big Data*, *NDR*, etc..
4	Falta de resiliencia en sistemas *OT*	Investigación en medidas correctivas basadas en métodos o mecanismos de restauración funcionando en tiempos óptimos (a ser posible en tiempo aproximadamente real). En caso de no poder retornar a un estado operativo similar al anterior a la manifestación del fallo, los sistemas deben permanecer en un estado seguro en el que no afecten a otros dispositivos empleados o servicios.

ANEXO I – RESULTADOS DE LA CONSULTA

	INVENTARIO	
	CARENCIA DE SEGURIDAD	**MEDIDAS COMPENSATORIAS**
1	Inexistencia de Inventarios.	Es necesario contar con herramientas de inventariado en tiempo real. Son especialmente interesantes los *BAD* descritos en la NISTIR 800-82r2 e incluidos en el modelo de referencia NIST1800-23 ya que, mediante la utilización de mecanismos pasivos, es decir, no intrusivos con el tráfico productivo, son capaces de realizar un inventariado de activos automático y en tiempo real. Estos sistemas además son capaces de identificar fabricante, *firmware*, número de serie, vulnerabilidades asociadas a la versión de *firmware* y sistemas operativos. Implantación de herramientas de auditoría automatizadas o semi-automatizadas que además se integren con herramientas de inventariado. De esta forma se dispondrá siempre de un inventariado actualizado de todos los activos existentes. Es recomendable, en la medida de lo posible, el mecanismo de inventariado se pueda obtener a partir del tráfico de red existente en la instalación. Realizar auditorías, para conocimiento de activos (Fabricante, Sistema Operativo, versión de hardware, versión de *firmware*, dirección *IP*, protocolo con el que se comunica, etc.). Todos estos datos se podrían obtener mediante *softwares* de mercado denominados *Industrial Anomaly Detection*. No se puede proteger aquello que se desconoce que se tiene.
2	Falta de control de instalación de dispositivos *IoT*.	Establecer un procedimiento de búsqueda de dispositivos a través del inventario exhaustivo de direcciones *IP*. Implantar procedimientos de control para la instalación de nuevos dispositivos. Vigilar los modelos de comunicación y asegurar los canales.

ANEXO I – RESULTADOS DE LA CONSULTA

	ARQUITECTURA DE RED	
	CARENCIA DE SEGURIDAD	**MEDIDAS COMPENSATORIAS**
1	Ausencia de definición de un diseño de arquitectura de seguridad de red para entornos *OT*.	Definición e implantación de un procedimiento que permita definir y regular un modelo de arquitectura base incluyendo la red *OT* y su relación con los entornos *IT*/corporativos. Aumentar las medidas de control físico y de acceso a redes. Reducir en la medida de lo posible las conexiones de equipos a más de una red. Incorporar sistemas de monitorización de red que permitan detectar intentos de acceso indebidos y cortafuegos donde sea posible. Concienciar y formar a operadores, ingenieros, desarrolladores y personal de mantenimiento. Establecimiento de procedimientos de acceso y uso de dispositivos de forma segura. En caso de que aplique/ establecer los accesos en la *DMZ*.
2	Falta de segmentación.	Realizar una segmentación, en la medida de lo posible teniendo en cuenta la norma de zonas de seguridad y conductos que propone la norma ISA99/IEC62443, con separación con cortafuegos de distintos fabricantes y respetando niveles Purdue. Además se deberá de crear una barrera *IT/OT* que incluyan varias *DMZ* donde se ubicarán los servidores de actualizaciones de firmas de los sistemas de seguridad *OT* y servidores de parches para los sistemas operativos generalistas existentes en la red *OT*. Una segunda *DMZ* se utilizará para crear máquinas de salto para dar acceso de forma segura a los telemantenedores. Uso de herramientas: Diodo de Datos, Cortafuegos, Control de acceso a red (*NAC*), *IDS/IPS* que soporten protocolos industriales. Uso estrictamente necesario de redes inalámbricas y solo si son seguras. Uso de mecanismos para la identificación de los dispositivos desplegados en el entorno para evitar la conexión de elementos no autorizados a la red. Implementar la segmentación de cada uno de las células de automatización en base a *switches* y *firewalls* industriales, ya que estos equipos están localizados en los armarios de fábrica, con sus correspondientes interferencias electromagnéticas, polvo, suciedad, etc.

ANEXO I – RESULTADOS DE LA CONSULTA

3	Inexistencia de una *DMZ IT/OT* En la arquitectura *OT* no existe una *DMZ IT/OT* en las plantas.	Esta *DMZ* es imprescindible ya que cumple con dos funciones: *1)* Albergar los sistemas de actualización de SO y *firmware* de los sistemas industriales 2) Red de acceso remoto seguro, donde se ubicarán máquinas de salto para realizar un telemantenimiento seguro.
4	Convergencia entre sistemas *IT* y *OT* Cada vez más se establecen relaciones y comunicaciones directas entre el mundo *IT* y el mundo *OT*. La diferencia de madurez a nivel de ciberseguridad de ambos mundos es abismal.	Deben de dotarse en los sistemas *IT* de soluciones que permitan protegerse contra ataques avanzados como *ransomware, antiphising, zero-days*, tanto a nivel de puesto de trabajo como a nivel de red, siendo deseable una gestión unificada y sencilla de los mismo. Gobierno de la Seguridad: Estructura, Roles, Funciones, Responsabilidades y procesos de gestión comunes o integrados, para el mundo *IT* y *OT*. Instalación de gestores de dominio *IT/OT* diferenciados que eviten en caso de la vulnerabilidad de uno de ellos, que el otro se vea vulnerado también. Abordar la integración de componentes de seguridad a nivel perimetral y a nivel de red, como *firewalls, IDS/IPS, VPN* y comunicación diodo. Establecer *VLANs* en *switches* de capa 3 y establecer *ACLs* entre diferentes segmentos de red. Aislar los puestos de control *OT* de salida internet y acceso a correo electrónico.
5	Falta de implementación de zonas y conductos en red *OT*.	Definición e implementación de segmentación de red *OT*.
6	Debilidades en los conductos entre capas de red.	Desarrollar una política de acceso que limite y controle los conductos habilitados entre capas. Vigilar especialmente los conductos que publican información del estado de variables y puntos de consigna.
7	Deficiencias de control de elementos activos de la red de operación.	Eliminar los administradores externos de *routers, switches* y *hubs* en la red de operación. Deshabilitar todos aquellos protocolos de red innecesarios en el sistema y limitar el uso de los mismos al mínimo (*hardening*).
8	Deficiencias de control de elementos de red, de uso corporativo.	Los subsistemas de control de acceso y videovigilancia, existentes en prácticamente todas las instalaciones industriales, suelen utilizar accesos a la red que pueden comprometer la seguridad de la misma, y por lo tanto se deberían establecer *VLANs* en *switches* de capa 3 y establecer *ACLs* entre el segmento de red de estos subsistemas de control de acceso y videovigilancia con el resto de redes.

ANEXO I – RESULTADOS DE LA CONSULTA

9	Deficiencias de control de elementos de comunicaciones inalámbricas.	Los subsistemas de conexión digital inalámbrica (*VHF*, satelital, *WIFI*, etc.) deben de contar con los mismos esquemas de control y de arquitectura que el resto de la red, para que no puedan comprometer la seguridad de la red.
10	Falta de documentación respecto a la topología de la red y protocolos de la misma.	Realizar auditoría para conocer cada uno de los componentes de red instalados en la fábrica y hacer una configuración de red detallada no solo con los componentes de red que existen, sino también sus IP y los distintos protocolos que se ejecutan entre cada uno de los componentes de la instalación. Todos estos datos se podrían obtener mediante software de mercado denominado *Industrial Anomaly Detection*.
11	Uso compartido de la *WIFI* corporativa.	Segregación de la *WIFI* para usos corporativos, de producción y personales. Implementación de medidas de control de acceso a redes *WIFI*, etc.

ANEXO I – RESULTADOS DE LA CONSULTA

	ANÁLISIS DE RED	
	CARENCIA DE SEGURIDAD	**MEDIDAS COMPENSATORIAS**
1.	Detección de anomalías en el tráfico.	Es recomendable la inclusión, en segmentos críticos, de sistemas de análisis de comportamiento y detección de anomalías (*BAD*), tal como indica la NIST 1800-23. Estos sistemas son los responsables de, recibiendo una copia del tráfico de la red, realizar una "foto" del estado de la planta incluyendo, protocolos, *SSOO*, fabricantes, modelo Purdue, inventariado de activos, descubrimiento de vulnerabilidades. Además, una vez se pasa el equipamiento a modo operacional, genera alarmas en base a: desviaciones del tráfico, cambio de protocolo, cambio de instrucción, *upgrade* de *firmware* de un *PLC*, *downgrade* de *firmware*, descarga de configuración, carga de configuración, un nuevo activo se descubra en la red.
2.	Ausencia de análisis de vulnerabilidades.	Establecer un mayor control de configuraciones, conexiones y actualizaciones de *software*. Incluir planes de acción para remediación.
3.	Ausencia de sistemas de gestión de eventos.	Integración de *SIEM* para el control de eventos y *logs* de sistema de aquellos sistemas que lo permitan.
4.	Se desconocen las vulnerabilidades existentes.	Aplicación de diagnósticos de vulnerabilidades.
5.	Ausencia de métodos efectivos para prevenir fugas de información.	Uso de herramientas *DLP* en los sistemas *OT* relacionados para el servicio con sistemas *IT*. Control / restricción de la información en dispositivos portátiles. Uso de herramientas *IRM (Information Right Management)*. Eliminación segura de información en dispositivos obsoletos. Restricciones de acceso externo desde la red industrial (uso de internet, *e-mail*, etc.). Normativa de uso de los medios.

ANEXO I – RESULTADOS DE LA CONSULTA

6.	Detección y tratamiento de incidentes de ciberseguridad incompletos.	Establecer procesos para la monitorización de eventos y detección, notificación y respuesta ante incidentes de ciberseguridad (*SIEM*, *SOAR*, etc.).
7.	Ausencia de monitorización de red	Además de la identificación de activos no inventariados la monitorización de red nos permite detectar anomalías (*BAD*) a través del análisis de los protocolos industriales en uso. El uso de *IDS/IPS* y *DPI* se puede completar con la integración de *honeypots*, *deceptions hosts*, etc.
8.	No realización de escaneo automático de vulnerabilidades.	Control de configuración, segmentación con *DMZ*, Control de conectividad indirecta, llave en cabinas, sistema de control de acceso a instalación y sala, Monitorización de red y *SIEM*.
9.	Automatización en las respuestas. Hasta la fecha las respuestas se basan en procedimientos manuales sin aún confiar en los sistemas *ICT* para liderar nuevas acciones y respuestas contra fallos, incidentes o ataques.	Investigación en mecanismos de respuesta automática o semi-automática para proporcionar prevención.
10.	Modelo y Herramientas para la identificación de Elementos críticos en la Infraestructura, sensibles a efectos en cascada que provoquen disrupciones graves del funcionamiento o servicio esencial.	Basarse en el Comité de Gestión de Resiliencia y Gestión integral de Riesgos. Posibles categorías sensibles: 1. Centros de control *SCADA*, monitorización. 2. Infraestructura tecnológica *IT* y *OT*. 3. Personal esencial- comité crisis, seguridad, emergencias, *O&M*, Sistemas y ciber...- incluidas subcontratas. 4. Procesos críticos de la instalación (operación, sistemas safety, logística, etc.). 5. Sistemas de Seguridad *security*. 6. Equipamientos y maquinarias esenciales (estación energía/cuadros eléctricos, sist. agua y gases, etc.). 7. Infraestructuras físicas (edificios y entorno geofísico, red de comunicaciones: carretera, tren, etc., poblaciones próximas y entornos naturales). 8. Servicios externos y suministros básicos. 9. Otros ámbitos específicos del Sector.

ANEXO I – RESULTADOS DE LA CONSULTA

	PROTOCOLOS DE RED	
	CARENCIA DE SEGURIDAD	**MEDIDAS COMPENSATORIAS**
1	Protocolos industriales en las comunicaciones entre controladores lógicos y sistemas de supervisión sin capacidad de mecanismos de control y/o cifrado.	Aumentar las medidas de control físico y a nivel de las redes. Concienciar y formar a operadores, ingenieros, desarrolladores y personal de mantenimiento. Dispositivos adicionales que permitan establecer mecanismos de control y cifrado.
2	Protocolos de comunicaciones industriales inseguros.	La medida ideal, pero la más complicada y la que lleva un periodo de implantación mucho más largo es que los fabricantes de Sistemas Industriales incorporen en sus soluciones protocolos seguros que incluyan cifrado por ejemplo. Incluir cifradores *HW* en las comunicaciones punto a punto. Estos cifradores no deben introducir latencias significativas. Incluir medidas de control del comportamiento de tráfico, de forma que, aunque no sea capaz de bloquear, sí que permita alertar de una anomalía de comportamiento en el tráfico de red.
3	Ausencia de políticas de control y procedimientos específicos para redes *OT* establecidos.	Definición de un *framework* de control que permita realizar una gestión efectiva del entorno *OT*.
4	Ausencia de seguridad en los múltiples protocolos de comunicación empleados por los dispositivos *OT*.	Empleo de arquitecturas basadas en *OPC UA* para la homogenización de las comunicaciones y el establecimiento de medidas de seguridad dentro de los protocolos empleados. Asegurar que el tráfico de comunicación entre los dispositivos y sus controladores/ se ejecute en un canal cifrado/ o en un micro segmento de red protegido.

ANEXO I – RESULTADOS DE LA CONSULTA

5	Desconocimiento de los protocolos *OT* usados para su posible protección.	Debido a que los protocolos *OT* no van cifrados, es recomendable evitar problemas de "*man in the middle*". Para ello, habrá que implantar soluciones como: uso de *VPNs* para comunicaciones a través de redes públicas, emplear *hardware* específico de seguridad que proteja la red local, utilizar sistemas de cifrado en las comunicaciones, utilizar doble factor de autenticación, etc.
6	Falta de estandarización general de la integración de sistemas *IT/OT* de manera segura. Hay pocos estándares que se centran en la integración de *IT* en entornos de *OT*, como es el caso del *IEC* 62351 (para entornos de energía), e incluso, si todos las tecnologías integradas siguen estándares específicos.	Estandarización a nivel nacional como internacional de la integración de tecnologías *IT* en entornos complejos de *OT*.

ANEXO I – RESULTADOS DE LA CONSULTA

	CONFIGURACIÓN	
	CARENCIA DE SEGURIDAD	**MEDIDAS COMPENSATORIAS**
1	Carencia de productos *OT* certificados en entorno *IT*. Equipos no certificados a nivel de ciberseguridad en la instalación.	Definición de protocolos y normas de certificación / Certificación de dispositivos industriales. Utilización de equipos diseñados bajo la premisa de Ciberseguridad y con garantías de mantenimiento de la misma durante el ciclo de vida del producto y a ser posible certificados, aunque como todos sabemos lo que hay que certificar en último término es el 100% de la instalación.
2	Utilización de sistema operativo de propósito general.	Implantación de una política de parcheo de los sistemas operativos de propósito general. Instalación de sistemas de seguridad reactivos que permitan realizar técnicas de parcheo virtual.
3	Carencias en copias de seguridad y en su gestión. Política de gestión de dispositivos los cuales sean susceptibles de conectar a la red *OT*. Ausencia o incorrecta gestión de *backups* centralizados (resiliencia).	Desarrollo e implantación de medidas cubriendo aspectos como planificación, copias remotas y pruebas de recuperación. Desarrollar e implantar un proceso de copias de seguridad, externas en la medida de lo posible, que asegure la existencia de copias para configuración, para *logs* de actividad y para *logs* de administración. En caso de ciberataque y *ransomware*, poder restaurar los sistemas desde un punto centralizado y con garantías de versionado.

ANEXO I – RESULTADOS DE LA CONSULTA

4	Existencia de configuraciones por defecto (puertos, contraseñas, etc.). Equipos de red no configurados correctamente. Existencia de Puntos muy sensibles. Deficiencias de control del *software* en la consola de operación. Deficiencias de control de versiones de *SW* y configuración de la consola de operación.	Desarrollo e implantación de políticas/ procedimientos técnicos de configuración y despliegue de tecnologías basada en necesidades que sustituya las configuraciones por defecto. Modificación de estructura de red para evitar el uso de equipos *dual home*. Establecer guías de bastionado de los dispositivos de red. Revisiones periódicas de la configuración. Identificación de esos puntos y creación de *DMZs*. Desarrollar un procedimiento para vigilar y evitar la instalación de aplicaciones no autorizadas, en particular ofimáticas (*Office, Chat*, etc.). Aparte del control de copias de seguridad, establecer un entorno de pruebas y un mecanismo de autorización de puesta en producción con segregación de funciones.
5	Servicios innecesarios en dispositivos *OT*. Configuraciones por defecto de dispositivos *ICS*. Carencia de bastionado de los equipos (por ejemplo, deshabilitar *USB*).	Deshabilitar protocolos: *Snmp; Telnet; UPnP, RDP, FTP*, etc., así como las conexiones que no sean estrictamente necesarias para el funcionamiento del sistema. Bloqueo de puertos. Eliminar/bloquear/cambiar cuentas y contraseñas por defecto. Bloquear servicios/ puertos, *plugins*, etc., no usados o inseguros. Uso de herramientas de gestión de la configuración. Deshabilitar recursos/procesos que no se requieren y aplicar medidas de bastionado.
6	Ausencia de sistemas de *Blacklist* o *Whitelist*. Falta de protección en el *End-Point*.	Configuración de *Blacklists* o *Whitelists* para denegar o permitir la ejecución de ciertos comandos en los sistemas. *Whitelisting* unido a diversas tareas de bastionado de la instalación.
7	Ausencia de gestión de flujos de trabajo autoservicio.	Configurar y diseñar el sistema de flujos para el autoservicio en las diferentes aplicaciones.
8	Deficiencias de control de continuidad de la operación.	Establecer un sistema de evaluación de riesgos, similar a los *BIAs*, para localizar debilidades de continuidad, ante fallos imprevistos en equipos, configuración de consola y *SW*.

ANEXO I – RESULTADOS DE LA CONSULTA

9	La falsa automatización de los procesos. Gestión automatizada de activos *IT/OT* y siguiendo modelos dinámicos específicos de gestión de identidad.	Existen muchos procesos que erróneamente se consideran automatizados, pues requieren de una administración, un control y unas gestiones adecuadas. Los procedimientos asociados a los procesos automáticos críticos deben documentarse adecuadamente e identificarse los roles que los supervisan. Diseño e implementación de modelos de gestión de identidad y *tracking* de activos existentes o nuevos.
10	Falta de integración de la seguridad en todas las etapas del desarrollo e implantación de nuevos sistemas y en los cambios. Medidas de seguridad no integradas en Dispositivos *ICS*, especialmente en aquellos de gama baja.	Establecer requerimientos de seguridad para los nuevos *ICS*. Integrar estos requerimientos en las distintas fases del desarrollo e implantación, así como en los cambios. Establecer un proceso de gestión de cambios en los *ICS*. Realizar evaluaciones de seguridad de los nuevos sistemas antes de su adquisición e implantación en producción. Uso de los paradigmas de seguridad *'Security by Design*', '*Privacy By Design*' y '*Security By Default´*.
11	Mala gestión de la confianza y la integridad.	La confianza debe establecerse en el entorno de arranque (*secure bootstrapping*) para que se pueda verificar la integridad del dispositivo desde el principio. Firmar el código de forma criptográfica para asegurar que no ha sido manipulado posteriormente y supervisar la ejecución del mismo para asegurar que no se ha sobrescrito. Permitir que un sistema vuelva a un estado que se sabía que era seguro.
12	Utilización de equipos *IT* en la parte *OT*, los cuales no están diseñados para aguantar los ambientes industriales.	Sustituir estos por equipos con hardware adecuado o trasladar a espacios adecuados y seguros físicamente, para conseguir una disponibilidad de la instalación a ser posible 24/7 pudiendo garantizar en la medida de lo posible la continuidad del negocio.
13	Protección *HW/SW* y "desde" sus diseños, conocido como "*security by design*", y afecta a la gran mayoría de dispositivos *OT*, los cuales presentan altas restricciones computacionales para gestionar recursos criptográficos (ej. *RTUs/PLCs*). Esto se debe considerar durante el diseño de estos componentes.	Contemplar medidas de protección a nivel *HW* como *TPM (Trusted Platform Module)* y *TEE (Trusted Execution Environment)* para crear un entorno de confianza ("root of trust"), arranque seguro y protección integra de los sistemas operativos. Para ello, también es fundamental abordar las actuales restricciones *HW/SW* de la mayoría de los controladores.

ANEXO I – RESULTADOS DE LA CONSULTA

	ACTUALIZACIONES Y OBSOLESCENCIA	
	CARENCIA DE SEGURIDAD	**MEDIDAS COMPENSATORIAS**
1	Dispositivos *legacy* sin capacidad de manejar identificaciones y/o autorizaciones en controladores lógicos (*PLCs, RTUs, DCS*).	Aumentar las medidas de control físico y a nivel de las redes. Concienciar y formar a operadores, ingenieros, desarrolladores y personal de mantenimiento. Establecimiento de procedimientos de acceso y uso de dispositivos legacy con condiciones de uso seguro. Ubicación de dispositivos legacy en segmentos de red aislados. Dispositivos adicionales que permitan manejar identificaciones y/o autorizaciones.
2	*Software* o *firmware* sin actualizar	Como medida compensatoria, se propone la utilización de mecanismos de parcheo virtual a nivel de red (dado que es muy complejo el poder instalar agentes por parte de soporte del fabricante los activos industriales). Estos mecanismos protegen a nivel de red a los activos afectados por las distintas vulnerabilidades, haciendo imposible su explotación. Es recomendable que este mecanismo no solo incluya firmas propietarias *IT* sino también firmas de protección propias de los sistemas industriales y que puedan añadirse firmas en formatos conocidos como *SNORT* o *YARA*. Acordar con el proveedor una estrategia y cronograma de implantación de parches. Establecer un plan de mitigación para cubrir la ausencia de parches críticos Además es recomendable la creación de *test-bed* o sistemas de pre-producción sobre los que probar el impacto de las actualizaciones de los sistemas asociados a los procesos industriales. Estos *test-bed* pueden ser bien físicos o bien virtuales. Encapsulamiento de sistemas operativos obsoletos tales como *Windows XP* o *Windows 7* mediante la virtualización de estos sistemas operativos. Uso de criptografía en los dispositivos para validación de nuevas versiones de software a través de firma digital en los procesos de actualización y evitar la manipulación de código. Establecer un sistema centralizado de gestionado de parches (*WSUS*) en el caso de que exista.

ANEXO I – RESULTADOS DE LA CONSULTA

3	Falta de soporte para la instalación de *endpoints* de seguridad en los sistemas *HMI*	Se debe de instalar en los sistemas de propósito general *endpoints* certificados por el fabricante de sistemas industriales que protejan contra ataques avanzados. Estos sistemas serán capaces de bloquear no solo contra amenazas conocidas sino también contra *zero days* o amenazas desconocidas.
4	Existencia de conexiones *WIFI* con *hardware* obsoleto que no permite desplegar mecanismos de seguridad (cifrado/ autenticación, etc.).	Sustitución de puntos de acceso por dispositivos que permitan un mayor nivel de seguridad. Implantación de sistemas *RADIUS*/ filtrados *MAC*. Empleo/ en la medida de lo posible de conexión cableada.
5	Deficiencias en la actualización de antivirus.	Acordar con el proveedor una estrategia y cronograma de implantación de antivirus. Establecer un plan de mitigación para cubrir los retrasos en la actualización. Proteger la capa más externa de la red con elementos de vigilancia, f*irewalls, IDEs* y similares.

ANEXO I – RESULTADOS DE LA CONSULTA

	TRAZABILIDAD, MONITORIZACIÓN	
	CARENCIA DE SEGURIDAD	**MEDIDAS COMPENSATORIAS**
1	Ausencia de registros de actividad en controladores lógicos (*PLCs*, *RTUs*, *DCS*).	Incorporar sistemas de monitorización y registro de actividad en la red. Incorporar sistemas de monitorización y registro de actividad en los sistemas que sea posible. Concienciar y formar a operadores, ingenieros, desarrolladores y personal de mantenimiento.
2	No se dispone de control sobre *reporting*.	Integración de un sistema de *reporting* para todo tipo de métricas y volumetría.
3	No se dispone de un sistema de escaneado de sistemas.	Configuración en integración de escáneres periódicos para mantener actualizado la integración de cuentas sobre los sistemas.
4	Ausencia de registro en la gestión de cambios en los sistemas.	Establecimiento de repositorios de registro e histórico de cambios.
5	Ausencia de sistema de registros de seguridad (accesos, conexiones externas, etc.).	Implantación de medidas de detección y registro automático descentralizado de cambios de seguridad y gestión de los mismos.
6	Falta de visibilidad del tráfico de red *OT*.	Instalación de sondas. Control de puertos y servicios *TCP/IP* abiertos inseguros y/o innecesarios, como pueden ser los puertos 23, 21 o 80, así como el uso de puertos *UDP* para realizar transacciones de control críticas. Establecer políticas de seguridad rigurosas, y planes de mantenimiento y de seguimiento frecuentes.

ANEXO I – RESULTADOS DE LA CONSULTA

7	Control rutinario de los servicios web, los cuales se establecen para realizar tareas de seguimiento en remoto o para la gestión administrativa. Muchas aplicaciones web pueden presentar deficiencias de seguridad que pueden liderar a múltiples tipos de ataques en remoto.	Establecer políticas de seguridad para verificar el código *Web* aplicado, establecer planes de seguimiento y monitorización de las aplicaciones web, y endurecer el acceso a la planta de control desde localizaciones remotas (incluida desde la red corporativa). Considerar la implantación de *WAF* (*Web Application Firewall*)
8	Auditoría, *accountability* (rendición de cuentas) y trazabilidad de acciones, especialmente en aquellos escenarios *OT* en el que haya federación de entidades, como puede ser los *Smart Grids*.	Adaptación de las nuevas tecnologías de tipo *Distributed Ledger Technologies (DLT)*, las cuales ofrecen inmutabilidad de los datos, seguridad y procedencia.

ANEXO I – RESULTADOS DE LA CONSULTA

	USO DE DISPOSITIVOS MÓVILES	
	CARENCIA DE SEGURIDAD	**MEDIDAS COMPENSATORIAS**
1	Deficiencias de control de equipos portátiles	Política de gestión de los dispositivos que sean susceptibles de ser conectados a la red *OT*. Limitar la posibilidad de que equipos portátiles se conecten a las redes *OT*. Vigilar cada conexión cableada. Implantar una política para impedir el acceso simultáneo a la red cableada y a la red *WIFI*. Robustecer la red *WIFI* de invitados. Los dispositivos no siempre tienen un identificador único que facilite el seguimiento, la supervisión y la gestión de los activos. El personal encargado de supervisar los hosts en la red, no necesariamente considera los dispositivos *IoT* como un *host* más. Se deben tener sistemas de rastreo que incluyan todos los activos por muy sencillos que sean, como por ejemplo los termostatos.
2	Utilización de equipos *IoT* de bajas prestaciones y sin medidas de ciberseguridad apropiadas.	Utilizar cuando sea posible componentes *IoT* y diseñados teniendo en cuenta la ciberseguridad y durante todo el ciclo de vida del producto. En los casos donde no sea posible deberán extremarse las medias de detección y control en el entorno de adquisición y en las infraestructuras de comunicaciones y en los sistemas de información de análisis de los datos adquiridos.
3	Aplicar políticas de *BYOD* sin considerar medidas preventivas y políticas de seguridad. De hecho, existen riesgos de infecciones por *USB* y por el autorun.inf.	Definir políticas de seguridad específicas para *BYOD* y revisar el estado actual de los dispositivos, pasando regularmente herramientas *anti-malware* o antivirus (ej. al inicio de la jornada), e instalar mecanismos de detección de intrusiones (principalmente basados en anomalías). También, es fundamental abordar planes de concienciación y formación en este aspecto.

ANEXO I – RESULTADOS DE LA CONSULTA

	CONCIENCIACIÓN, PERSONAL, FORMACIÓN	
	CARENCIA DE SEGURIDAD	**MEDIDAS COMPENSATORIAS**
1	Falta de cultura de seguridad en el mundo *OT*.	Establecer políticas de empresa de formación y concienciación.
2	Formación específica para empleados y usuarios.	Impartición de cursos específicos y regulares con registro de asistencia a los empleados/operadores de las infraestructuras/sistemas.
3	Formación de los perfiles técnicos de operación *OT* en competencias *IT*.	Capacitación específica en las carencias identificadas.
4	Formación de los perfiles técnicos de operación *IT* en competencias *OT*.	Capacitación específica en las carencias identificadas.
5	No disponer de un responsable de ciberseguridad *OT* dedicado y personal formado para atender las necesidades del área.	Asignar dicha responsabilidad.
6	No realización de simulacros de intrusión avanzada (*Red Team*) combinando vectores físicos, digitales e ingeniería social.	Realización de un tests de intrusión periódicos y ejercicios de coordinación de respuesta en caso de crisis.
7	Inexperiencia en respuesta a incidentes de ciberseguridad.	Contar con un servicio bajo demanda de apoyo en respuesta a incidentes de ciberseguridad.

ANEXO I – RESULTADOS DE LA CONSULTA

	SEGURIDAD FÍSICA	
	CARENCIA DE SEGURIDAD	**MEDIDAS COMPENSATORIAS**
1	Insuficiente aislamiento de los sistemas de control.	Implantación de medidas de control, tanto físicas como lógicas para restringir los accesos (p.e. servidores "enjaulados").
2	Sistemas de control de acceso inseguros.	Asegurar que el cableado y acceso a equipos críticos se encuentra protegido y seguro. Establecer controles de acceso (acceso contraseña/ llaves/ o acceso biométrico) a los sistemas críticos. Registro de histórico de accesos físicos al centro de control de los sistemas (logs de acceso/ grabaciones de videovigilancia). Identificación visual de la restricción de acceso a áreas críticas.
3	Falta de control de la consola de administración.	Ubicar la consola de administración en la Sala de Control. Implantar un sistema de logs de tipo *SIEM*.
4	Deficiencias en el acceso físico a la red de operación.	Implantar una separación y distancia entre las redes de control y la red corporativa que dificulte la conexión errónea o maliciosa entre redes.
5	Deficiencias en el control del acceso físico a las instalaciones.	El acceso a los lugares en los que existan dispositivos activos (sala de control, sala de *PLCs*, actuadores y sensores, salas de comunicaciones, torres y *Shelters* de comunicaciones etc.) debe ser restringido y controlado adecuadamente.
6	Ausencia de medidas de seguridad en dispositivos especialmente sensibles.	Catalogación de dispositivos sensibles. Aislamiento, control de acceso, alarma en cabinas y posibles rondas en casos excepcionales.
7	Falta de control en sistemas *CCTV*	Revisión periódica de los sistemas *CCTV*. Establecer un procedimiento para la protección de datos.

ANEXO I – RESULTADOS DE LA CONSULTA

	GESTIÓN DE PROVEEDORES	
	CARENCIA DE SEGURIDAD	**MEDIDAS COMPENSATORIAS**
1	Proveedores únicos o monopolio.	Identificar a los proveedores únicos y exigirles medidas adicionales. Diversificar proveedores.
2	Productos sin medidas de seguridad de fábrica.	Políticas de comprobación e implantación de seguridad en productos adquiridos. Testeo de seguridad de los productos adquiridos. Establecer medidas de seguridad de red a nivel de detección y protección.
3	Falta de procedimiento en la contratación de productos y servicios con especial atención a la cadena de suministros.	Procedimientos contractuales sólidos y revisados periódicamente por el cliente.

ANEXO I – RESULTADOS DE LA CONSULTA

	ESTRATEGIAS	
	CARENCIA DE SEGURIDAD	**MEDIDAS COMPENSATORIAS**
1	Laboratorios *OT* donde testar la vulnerabilidad de los equipos *OT* en redes *IT*.	Diseño e implementación de laboratorios propios o de terceros.
2	Requerimientos de seguridad en la adquisición de dispositivos.	Establecimiento y aplicación de una *baseline* de requisitos de seguridad según estándares como *IEC-62443-33* que formen parte de los procesos de adquisición tecnológica.
3	No disponer de un plan de continuidad de negocio implementado.	Haber realizado el *BIA* y aplicado alguna medida de contingencia esencial.
4	Falta de revisiones regulares de hacking ético frecuentes de toda la infraestructura.	Realización de al menos un análisis anual de vulnerabilidades a las infraestructuras más críticas.
5	La gestión de crisis y su comunicación asociada.	La gestión de crisis es uno de los aspectos primordiales a la hora de abordar escenarios complejos relacionados con fallos de seguridad. Su plan de comunicación asociado es vital. Desarrollar un adecuado Plan de Crisis e integrarlo en toda la organización y todos los sistemas críticos es vital. A la hora de su desarrollo el Plan de comunicación y el árbol de toma de decisiones escrítico.
6	Análisis del Impacto de los Sistemas en el Negocio.	En multitud de ocasiones se realizan grandes inversiones en protección de la información y la salvaguarda de sus activos. Sin embargo estas inversiones no están soportadas por un análisis riguroso del impacto en el negocio. Sistemas que pueden ser considerados como no críticos a priori, después de un análisis pueden realmente causar un impacto a la organización muy importante. Es esencial realizar un análisis de impacto.
7	Documentación apropiada de sistemas y su configuración.	Los sistemas y su configuración asociada deben de documentarse adecuadamente. Las guías de protección aplicadas (*Security Guidelines*) y su cumplimiento deben ser apropiadamente descritas. Deben establecerse requisitos estrictos en esta materia, especialmente para los sistemas más críticos.

ANEXO I – RESULTADOS DE LA CONSULTA

8	Los datos no es el aspecto critico de los sistemas.	En muchos casos la seguridad de la información no está construida en base a la criticidad de los datos asociados a los sistemas. Se realizan muchas inversiones en seguridad, pero no siempre están focalizadas en la protección de los datos almacenados o en tránsito. Es primordial proteger ambas partes de los sistemas: los repositorios y las comunicaciones.
9	Ausencia Responsabilidades de Seguridad definidas o poco claras en el mundo *OT*.	Creación de roles y responsabilidades de seguridad específicos para *OT* (*OT Security Managers*), dependientes de un rol común integrador de la Seguridad *IT/OT* (*CSO, CISO*, etc.).
10	Ausencia de objetivos de seguridad establecidos.	Establecer los objetivos de mejora de la seguridad de forma periódica. Planificar y asignar recursos para la consecución de los objetivos marcados. Establecer indicadores de evolución de la consecución de dichos objetivos.
11	Ausencia de Normas de Seguridad internas o de conocimiento de las mismas por el personal.	Identificación de la normativa aplicable. Establecer un Marco Normativo Interno de seguridad integrando *IT* y *OT* (políticas, normas y procedimientos). Considerar el Marco general para *OT*, y el específico para cada sector (da lugar a varios módulos verticales y horizontales). Difusión del Marco Normativo al personal implicado.
12	Falta de una clasificación y criticidad de la información e *ICS* formal y las medidas a aplicar.	Establecer una norma y procedimientos para la clasificación y criticidad de la información e *ICS*.
13	Ausencia de Gestión del Riesgo	Realización de *AARR* periódicos (anuales) o cuando haya cambios relevantes. Establecimiento de criterios de aceptación del riesgo. Realización de Plan de Tratamiento del Riesgo (PTR) / Plan Director de Seguridad (PDS).

ANEXO I – RESULTADOS DE LA CONSULTA

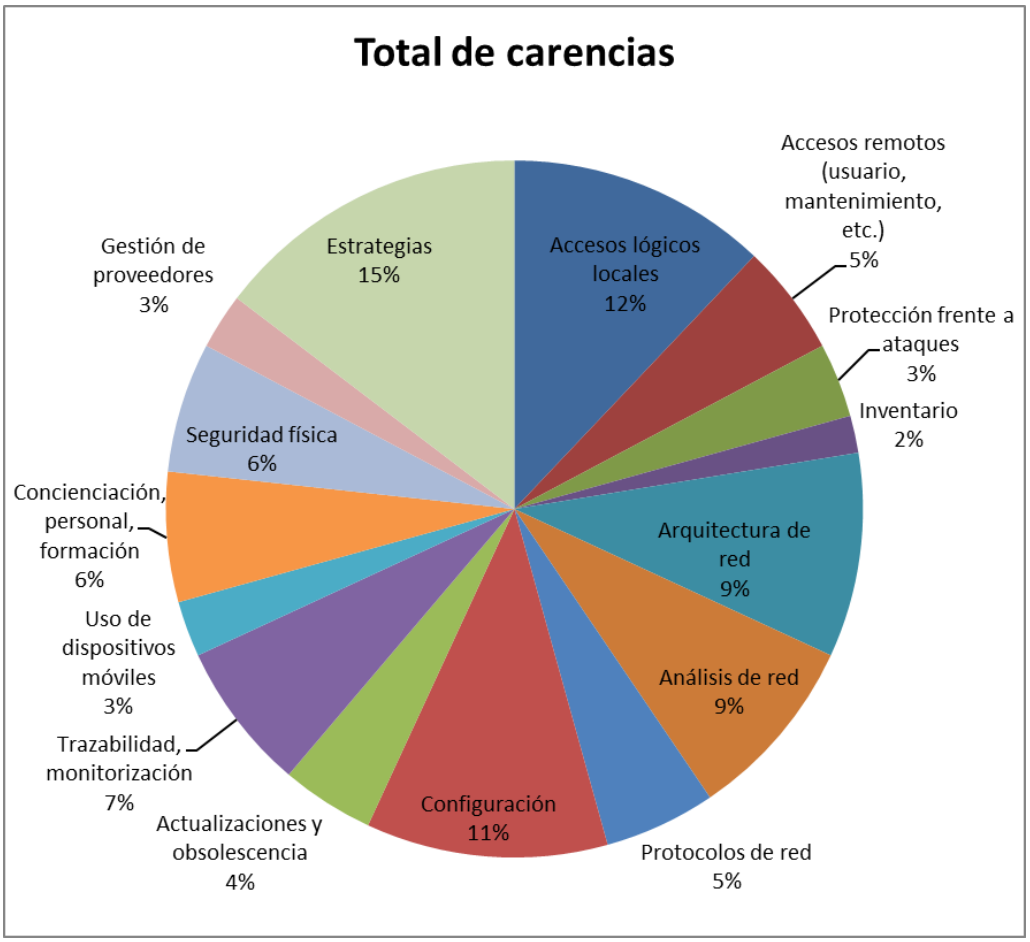
14	Falta de control de toda la cadena de suministro y complejidad de la misma.	Establecimiento de un proceso de Identificación, Evaluación y Gestión de proveedores. Identificación de interdependencias. Realización de *AARR* en la cadena de suministro. Sistema de Gestión de la cadena de suministro. Acuerdo con proveedores incluyendo seguridad (lógica, física y de las personas). Acuerdos de Nivel de Servicio (ANS). Establecer los requisitos de seguridad mínimos a cumplir por los proveedores.
15	Falta de conocimiento y control de Estado de la Seguridad y el Cumplimiento.	Establecimiento de un Marco de Controles. Proceso de Gestión del cumplimiento (implantación y revisión). Cuadro de Mando de Seguridad Integral. Establecer un plan de auditorías periódicas de Cumplimiento y Análisis de Vulnerabilidades y Planes para la corrección de las debilidades encontradas. Uso de herramientas de detección pasiva de vulnerabilidades. Establecer procesos de inteligencia de amenazas: detección de amenazas internas y externas. Uso de herramientas *GRC-IRM* para el Gobierno y Gestión de la Seguridad Integral.
16	Ausencia de Planes de Continuidad del Negocio formales.	Ausencia de Planes de Continuidad del Negocio formales. Realización de un análisis de impacto de negocio (*BIA)* para identificar los procesos críticos. Planes de Continuidad del Negocio. Planes de Gestión de Crisis. Normas y Procedimientos de Copias y recuperación de la información.
17	Falta de estudio de negocio en los sistemas y servicios relacionados con la Ciberseguridad.	Realizar auditoría para saber dónde estamos, dónde queremos llegar y un plan de cómo llegar al punto final, para poder hacer un presupuesto y poder discutirlo y aprobarlo con la dirección de la compañía.

ANEXO II – ESTADÍSTICAS

En forma de resumen, de las entidades consultadas se recabaron las siguientes carencias:

ÁMBITO	Nº CARENCIAS
Accesos lógicos locales	14
Accesos remotos (usuario, mantenimiento, etc.)	6
Protección frente a ataques	4
Inventario	2
Arquitectura de red	11
Análisis de red	10
Protocolos de red	6
Configuración	13
Actualizaciones y obsolescencia	5
Trazabilidad, monitorización	8
Uso de dispositivos móviles	3
Concienciación, personal, formación	7
Seguridad física	7
Gestión de proveedores	3

ANEXO II – ESTADÍSTICAS



ANEXO II – ESTADÍSTICAS

Número de entidades que han detectado carencias para cada ámbito:

	PARTICIPACIÓN POR ENTIDADES			
ÁMBITO	CONSULTORA	ASOCIACIÓN	UNIVERSIDAD	FABRICANTE
Accesos lógicos locales	2	2	0	3
Accesos remotos (usuario, mantenimiento, etc.)	1	0	0	4
Protección frente a ataques	0	1	1	3
Inventario	1	1	0	4
Arquitectura de red	2	2	1	5
Análisis de red	1	0	2	5
Protocolos de red	2	1	1	3
Configuración	2	2	1	4
Actualizaciones y obsolescencia	1	2	2	5
Trazabilidad, monitorización	1	2	1	2
Uso de dispositivos móviles	0	1	1	2
Concienciación, personal, formación	1	2	1	1
Seguridad física	2	1	0	2
Gestión de proveedores	2	1	0	5
Estrategias	1	1	1	5

ANEXO II – ESTADÍSTICAS

Representación en tanto por ciento de las entidades que han detectado carencias para cada ámbito, en relación con el número total de colaboradores de cada grupo:

	REPRESENTACIÓN POR ENTIDADES			
ÁMBITO	CONSULTORA	ASOCIACIÓN	UNIVERSIDAD	FABRICANTE
Accesos lógicos locales	100%	50%	0%	50%
Accesos remotos (usuario, mantenimiento, etc.)	50%	0%	0%	67%
Protección frente a ataques	0%	25%	50%	50%
Inventario	50%	25%	0%	67%
Arquitectura de red	100%	50%	50%	83%
Análisis de red	50%	0%	100%	83%
Protocolos de red	100%	25%	50%	50%
Configuración	100%	50%	50%	67%
Actualizaciones y obsolescencia	50%	50%	100%	83%
Trazabilidad, monitorización	50%	50%	50%	33%
Uso de dispositivos móviles	0%	25%	50%	33%
Concienciación, personal, formación	50%	50%	50%	17%
Seguridad física	100%	25%	0%	33%
Gestión de proveedores	100%	25%	0%	83%
Estrategias	50%	25%	50%	83%

ANEXO III – ADAPTACIÓN DE LAS AMENAZAS DEL CATÁLOGO MAGERIT A ENTORNOS OT

En base a la categorización realizada en el catálogo de amenazas MAGERIT – versión 3.0, existen cuatro tipologías de origen:

- Ataques intencionados.
- Desastres naturales.
- Errores y fallos no intencionados.
- De origen industrial.

Las amenazas identificadas a continuación se podrían duplicar, si fuera preciso, con el fin de establecer afectaciones diferentes en función del ámbito donde se puedan presentar dichas amenazas.

A.3	**Manipulación de los registros de actividad**	Los registros que en segundo plano crean las aplicaciones del ámbito *OT* no pueden garantizar su integridad por motivos técnicos u organizativos establecidos, impidiendo establecer imputabilidad.
A.4	**Manipulación de la configuración**	Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.
A.5	**Suplantación de la identidad de usuario**	Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Es importante analizar el tipo de privilegios que implica la identidad suplantada y si la suplantación se ha producido en local o remoto.
A.6	**Abuso de privilegios de acceso**	Privilegio es una autorización especial otorgada a un usuario en particular para realizar operaciones de relevantes. El abuso de una cuenta privilegiada ocurre cuando se utilizan los privilegios asociados al usuario de forma inapropiada o fraudulenta, ya sea, con intencionalidad, de forma accidental o por ignorancia de los procedimientos.
A.7	**Uso no previsto**	Utilización de recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.
A.8	**Difusión de *software* dañino**	Propagación intencionada de virus, *spyware*, gusanos, troyanos, ataques *DDOS* o *ramsomware* entre las principales categorías de *software* dañinos. Mención especial requiere el entorno Cloud mediante el cual un ataque puede afectar significativamente la actividad empresarial. Además del entorno *Cloud*, también habría que señalar aquellos ataques que proceden de la cadena de suministro.
A.9	**Re-Encaminamiento de mensajes**	Envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a dónde o por dónde no es debido. Puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Un atacante puede forzar un mensaje para circular a través de un nodo determinado de la red donde puede ser interceptado. Es particularmente destacable el caso de que el ataque de encaminamiento lleve a una entrega fraudulenta, acabando la información en manos de quien no debe.

ANEXO III – ADAPTACIÓN DE LAS AMENAZAS DEL CATÁLOGO MAGERIT A ENTORNOS OT

A.10	**Alteración de secuencia**	Alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando a la integridad de los datos afectados o a las actuaciones realizadas.
A.11	**Acceso no autorizado**	El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del proceso de autorización o del sistema de control de acceso.
A.12	**Análisis de tráfico**	El atacante sin necesidad de entrar a analizar el contenido de las comunicaciones es capaz de extraer conclusiones a partir del origen, destino, metadatos, volumen y frecuencia de los intercambios.
A.13	**Repudio**	Negación a posteriori de actuaciones o compromisos adquiridos en el pasado. Repudio de origen: Negación de ser el remitente u origen de un mensaje o comunicación. Repudio de recepción: Negación de haber recibido un mensaje o comunicación. Repudio de entrega: Negación de haber recibido un mensaje para su entrega a otro.
A.14	**Interceptación de información (escucha)**	El atacante llega a tener acceso pasivo a información que no le corresponde, sin que la información en sí misma se vea alterada.
A.15	**Modificación de la información**	Alteración intencional de la información, con ánimo de obtener beneficio o causar un perjuicio.
A.18	**Destrucción de información**	Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio. Señalar la creciente migración de la información a entornos *cloud* con lo que ello significa respecto a los soportes clásicos.
A.19	**Divulgación de información**	Revelación de información relevante de forma deliberada.
A.22	**Manipulación de programas**	Alteración intencionada del funcionamiento de programas y *firmware*, persiguiendo un beneficio indirecto cuando se utilice.
A.23	**Manipulación de equipos**	Alteración intencionada del funcionamiento de los equipos, persiguiendo un beneficio indirecto cuando cuando se utilice.
A.24	**Denegación de servicio**	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
A.25	**Robo**	La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, indisponibilidad. El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales.
A.26	**Ataque destructivo**	Sabotaje, vandalismo, terrorismo, acción militar, etc.
A.27	**Ocupación enemiga**	Cuando los locales han sido invadidos y se carece de control sobre los propios medios de trabajo.

ANEXO III – ADAPTACIÓN DE LAS AMENAZAS DEL CATÁLOGO MAGERIT A ENTORNOS OT

A.28	**Indisponibilidad de personal**	Ausencia deliberada del puesto de trabajo: Huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos, etc.
A.29	**Extorsión**	Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.
A.30	**Ingeniería social**	Recopilación de información personal, sin el uso de la tecnología.
A.31	**Indisponibilidad de proveedores**	Ausencia deliberada de un proveedor: Huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos, etc. Esta tipología de ataque afecta directamente a la cadena de suministro.
A.32	**Indisponibilidad de edificios / Instalaciones (A)**	Indisponibilidad de edificios / Instalaciones por ataques intencionados de origen interno o externos

DESASTRES NATURALES		
N.1	Todo aquel fenómeno natural peligroso para el sistema.	Existe una gran variedad dentro de las posibles categorías, tales como atmosférico, hidrológico, sísmico, volcánico o incendios. Algunos ejemplos concretos serían huracanes, tormentas, sequía, erosión, inundaciones, tsunamis, fallas, flujos de lava, hundimientos o incendios, frio o calor extremos, etc.

ANEXO III – ADAPTACIÓN DE LAS AMENAZAS DEL CATÁLOGO MAGERIT A ENTORNOS OT

ERRORES Y FALLOS NO INTENCIONADOS		
E.1	**Errores de los usuarios**	Equivocaciones de las personas cuando usan los servicios o los sistemas.
E.2	**Errores del administrador**	Equivocaciones de las personas con responsabilidades de instalación y operación.
E.3	**Errores en la monitorización**	• equipos no monitorizados • equipos no autorizados • medidas no monitorizadas • entradas / salidas no monitorizadas (de pdi) • *input data, output data, intermediate data*
E.4	**Errores en la configuración**	• servicios autorizados • flujos autorizados (*routing*) • protocolos autorizados • [formatos de] datos autorizados • cuentas de usuario no autorizadas (por defecto, personal ausente,…) • arquitectura del sistema (zonas y conducciones) • certificados (validación de firmas) • bastionado (fortificación) configuración [de seguridad]
E.7	**Deficiencias en la organización**	Cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión. Acciones descoordinadas, errores por omisión, etc.
E.8	**Difusión de *software* dañino**	Propagación inocente de virus, *spyware*, gusanos, troyanos, ataques *DDOS* o *ramsomware* entre las principales categorías de *software* dañinos. Mención especial requiere el entorno *Cloud* mediante el cual un error puede afectar significativamente la actividad empresarial. Además del entorno *Cloud*, también habría que señalar aquellos errores que proceden de la cadena de suministro.
E.9	**Errores de re-encaminamiento**	Envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a dónde o por dónde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando información en manos de quien no se espera.
E.10	**Errores de secuencia**	Alteración accidental del orden los mensajes transmitidos.

ANEXO III – ADAPTACIÓN DE LAS AMENAZAS DEL CATÁLOGO MAGERIT A ENTORNOS OT

E.15	**Alteración de la información**	Alteración accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático.
E.18	**Destrucción de información**	Pérdida accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas. Señalar la creciente migración de la información a entornos *cloud* con lo que ello significa respecto a los soportes clásicos.
E.19	**Divulgación de información**	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel, etc. La información llega accidentalmente a personas que no deberían tener conocimiento de ella. Señalara la creciente migración de la información a entornos *cloud* con lo que ello significa respecto a los soportes clásicos.
E.20	**Vulnerabilidades de los programas**	Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario, pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.
E.21	**Errores de mantenimiento / actualización de programas**	Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.
E.22	**Errores de mantenimiento / actualización de equipos**	Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso
E.24	**Caída del Sistema por agotamiento de recursos**	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
E.25	**Pérdida de equipos**	La pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de información los más habituales. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.
E.28	**Indisponibilidad de personal (pandemia y otros)**	Ausencia accidental del puesto de trabajo: pandemia Sars Covid19, alteraciones del orden público, guerra bacteriológica, fuga de gas, accidente, etc.
E.29	**Indisponibilidad Edificios/Instalaciones [E]**	Indisponibilidad de edificios o instalaciones por errores y fallos no autorizados. Puede separarse por edificios o instalaciones clave.

ANEXO III – ADAPTACIÓN DE LAS AMENAZAS DEL CATÁLOGO MAGERIT A ENTORNOS OT

ORIGEN INDUSTRIAL		
I.1	**Fuego**	Incendios: Posibilidad de que el fuego acabe con recursos de los sistemas industriales. Se puede separar esta amenaza por edificios o instalaciones clave.
I.2	**Daños por agua**	Escapes, fugas, inundaciones: posibilidad de que el agua acabe con recursos de los recursos de los sistemas industriales.
I.3	**Contaminación mecánica**	Vibraciones, polvo, suciedad, etc.
I.4	**Contaminación electromagnética**	Interferencias de radio, campos magnéticos, luz ultravioleta, etc.
I.5	**Avería de origen físico o lógico**	Fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento de los sistemas industriales. En sistemas de propósito específico, a veces es difícil si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.
I.6	**Corte del suministro eléctrico**	Cese de la alimentación de potencia.
I.7	**Condiciones inadecuadas de temperatura y/o humedad**	Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frio, exceso de humedad.
I.8	**Fallo de servicios de comunicaciones**	Cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios de transporte, detención o simple incapacidad para atender al tráfico presente.
I.9	**Interrupción de otros servicios o suministros esenciales**	Otros servicios o recursos de los que depende la operación de los equipos, por ejemplo, papel para las impresoras, tóner, refrigerante, …
I.10	**Degradación de los soportes de almacenamiento de la información**	Como consecuencia del paso del tiempo o condiciones físicas como temperatura, humedad, presión, etc. Señalar la creciente migración de la información a entornos *cloud* con lo que ello significa respecto a los soportes clásicos.
I.11	**Emanaciones electromagnéticas**	Hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque. Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información.
I.12	**Indisponibilidad de edificios / Instalaciones (I)**	Indisponibilidad de edificios o instalaciones por accidentes de origen industrial.

ANEXO IV - GLOSARIO DE TÉRMINOS

ACL:	*Access Control List*
ANS:	Acuerdo de Nivel de Servicio
BAD:	*Behavioral analytics and anomaly detection*
BIA:	*Business Impact Analysis*
BYOD:	*Bring Your Own Device*
CISO:	*Chief Information Security Officer*
CSIRT:	*Computer Security Incident Response Team*
CSO:	*Chief Security Officer*
DCS:	*Distributed Control System*
DDOS:	*Distributed Denial of Service*
DLP:	*Data Loss Prevention*
DLT:	*Distributed Ledger Technologies*
DMZ:	*Demilitarized Zone*
DOS:	*Denial of Service*
EDR:	*Endpoint Detection and Response*
ENS:	Esquema Nacional de Seguridad
ERP:	*Enterprise Resource Planning*
FW:	*Firewall*
GDPR:	Reglamento General de Protección de Datos (2016/679)
GRC:	Gobernabilidad, Riesgo y Cumplimiento
HMI:	*Human-Machine Interface*
HW:	Hardware
I+D:	Investigación + Desarrollo
IA:	Inteligencia Artificial
ICS:	*Industrial Control Systems*
IDS:	*Intrusion Detection System*
IEC:	*International Electrotechnical Commission*

ANEXO IV - GLOSARIO DE TÉRMINOS

IoT:	*Internet Of Things*
IP:	*Internet Protocol*
IPS:	*Intrusion Prevention System*
IRM:	*Information Rights Management*
ISA:	*International Society of Automation*
ISO:	*International Organization for Standardization*
IT:	*Information Technology*
LAN:	*Local Area Network*
MES:	*Manufacturing Execution System*
NAC:	*Network Access Control*
NGFW:	*Next-Generation Firewall*
NIS:	*Network and Information Systems*
NIST:	*National Institute of Standards and Technology*
O&M:	*Operation and Maintenance*
OPC UA:	*Open Protocol Communication Unified Architecture*
Orden PCI:	Orden Presidencia Relaciones con las Cortes e Igualdad
OSE:	Operador de Servicio Esencial
OT:	*Operation Technology*
PbD:	*Privacy by Design*
PDS:	Plan Director de Seguridad
PERA:	*Purdue Enterprise Reference Architecture*
PIC:	Protección de Infraestructuras Críticas
PLC:	*Programmable Logic Controller*
PTR:	Plan de Tratamiento del Riesgo
RBAC:	*Role Based Access Control*
RD:	Real Decreto
RTU:	*Remote Terminal Unit*

ANEXO IV - GLOSARIO DE TÉRMINOS

SCADA:	*Supervisor Control and Data Acquisition*
SCI:	Sistema de Control Industrial
SIEM:	*Security Information and Event Management*
SO:	Sistema Operativo
SOAR:	*Security Orchestration, Automation and Response*
SW:	Software
TCP/IP:	*Transmission Control Protocol/Internet Protocol*
TEE:	*Trusted Execution Environment*
TIC:	Las Tecnologías de la Información y las Comunicaciones
TPM:	*Trusted Platform Module*
UE:	Unión Europea
UPnP:	*Universal Plug and Play*
USB:	*Universal Serial Bus*
VHF:	*Very High Frequency*
VLAN:	*Virtual Local Area Network*
VPN:	*Virtual Private Network*
WIFI:	*Wireless Fidelity*
WSUS:	*Windows Server Update Services*

GUÍA SOBRE CONTROLES DE SEGURIDAD EN SISTEMAS OT

isms forum INTERNATIONAL INFORMATION SECURITY COMMUNITY

OCC OFICINA DE COORDINACIÓN DE CIBERSEGURIDAD

GOBIERNO DE ESPAÑA MINISTERIO DEL INTERIOR

Anexo 3: Ciberseguridad en dispositivos IIoT (.pdf)

Ciberseguridad en dispositivos IIoT

En este apartado se detallan exhaustivamente los requisitos que deben cumplir los equipos IIoT integrados en la infraestructura de Aigües de Barcelona, tras analizar las posibles amenazas que podrían afectar al nuevo sistema de adquisición de datos IIoT de Aigües de Barcelona.

Para ello, se ha utilizado la metodología STRIDE, que permite identificar y categorizar las posibles amenazas en seis categorías diferentes: *Spoofing*, *Tampering*, *Repudiation*, *Information Disclosure*, *Denial of Service* y *Elevation of Privilege*.

A partir de este análisis, se han establecido una serie de requerimientos que los equipos IIoT deben cumplir para garantizar la seguridad y la integridad de la infraestructura de Aigües de Barcelona. Estos requerimientos incluyen medidas de autenticación y autorización, controles de acceso, cifrado de datos, integridad de los datos y monitorización constante de la red.

Lo que se indica en este apartado es esencial para asegurar que los equipos IIoT integrados en la infraestructura de Aigües de Barcelona cumplan con los estándares de seguridad necesarios para proteger la red y los datos adquiridos a través del sistema de adquisición de datos IIoT.

1. Análisis STRIDE

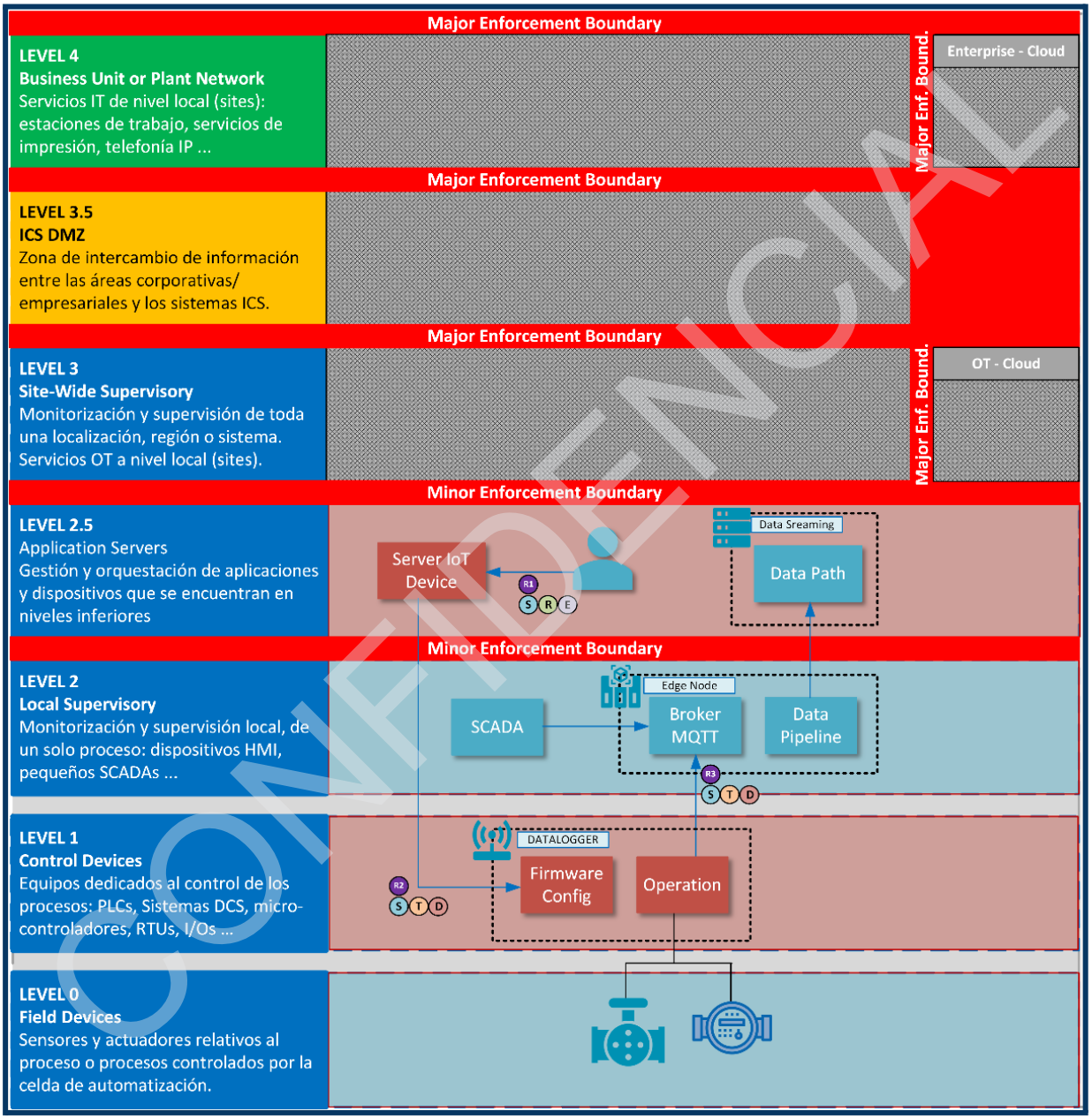
Se ha realizado el análisis de tres arquitecturas de red en la que intervienen dispositivos IIoT, sobre ellas se han identificado las posibles amenazas que pueden afectar al correcto funcionamiento del sistema.

En la siguiente tabla se visualizan los identificadores que se han colocado sobre las comunicaciones en los esquemas de las arquitecturas, junto con las amenazas, la dimensión a la que afecta cada una de ellas y una breve descripción de las mismas.

Identificador	Amenazas	Dimensión afectada	Descripción
S	*Spoofing*	Autenticación	Suplantar una entidad de confianza a través de la falsificación de los datos en una comunicación.
T	*Tampering*	Integridad	Alterar los datos enviados en una comunicación de confianza mediante un *Man-In-The-Middle* o un *Replay Attack* que permita alterar los valores del sistema.
R	*Repudiation*	No repudio	Modificar la comunicación para evitar que se almacene el origen y la fecha en la que se ha realizado.
I	*Information disclosure*	Confidencialidad	Observar los datos enviados en una comunicación de confianza mediante un *Man-In-The-Middle*.
D	*Denial of service*	Disponibilidad	Saturar la red para evitar el funcionamiento o la comunicación de los servicios con otros. El ciberdelincuente puede conseguirlo mediante *Man-In-The-Middle* o aprovechando alguna vulnerabilidad del sistema.
E	*Elevation of privilege*	Autorización	Obtener privilegios de usuarios diferentes a los que posee el usuario que se conecta obteniendo las credenciales de acceso de otro usuario o explotando alguna vulnerabilidad del sistema.

Dispositivo IIoT publicando datos en Edge

El siguiente esquema representa la integración de un sistema IIoT integrado en una instalación en la que se dispone de un dispositivo Edge. En este caso los datos se suben a los niveles superiores siguiendo el estándar de flujo de datos de Aigües de Barcelona, es decir, a través del *Edge*. Para ello, el equipo IIoT publica toda la información en un bróker MQTT que se encuentra en ejecución en el *Edge*. Tras esto, el *Edge* se encarga de subir los datos al *Data Streaming* del nivel superior siguiendo los estándares de la arquitectura IIoT de Aigües de Barcelona.



Esta arquitectura presenta tres riesgos cibernéticos, en ninguno de ellos preocupa la revelación de la información ya que la confidencialidad no es una dimensión primordial en los sistemas de control industrial.

R1: Este riesgo se produce en el acceso a la aplicación web utilizada para actualizar el *firmware* o configurar los dispositivos IIoT. Las amenazas posibles son las siguientes:

- *Spoofing* [S]: Un usuario no autorizado podría acceder a la aplicación web, explotando alguna vulnerabilidad de la misma, usando técnicas de fuerza bruta u obteniendo las credenciales de un usuario legítimo. Una vez ha accedido a la aplicación podría realizar el alta de nuevos dispositivos, desplegar nuevas configuraciones o modificar las existentes.
- *Repudiation* [R]: Un usuario que accede a la aplicación podría realizar el alta o/y la modificación de las configuraciones. Con el objetivo de ocultar las acciones realizadas y dificultar la investigación forense podría modificar o eliminar los registros de auditoría, y de esta forma negar las mismas.
- *Elevation of privileges* [E]: Un usuario que accede a la aplicación con permisos mínimos podría ampliarlos explotando alguna vulnerabilidad de la aplicación o encontrando una forma de acceder con un usuario que posea mayor rango de permisos para realizar acciones que no le están permitidas.

R2: Este riesgo se produce en la comunicación de la aplicación del fabricante con los dispositivos IIoT. Las amenazas que se podrían materializar en el canal son las siguientes:

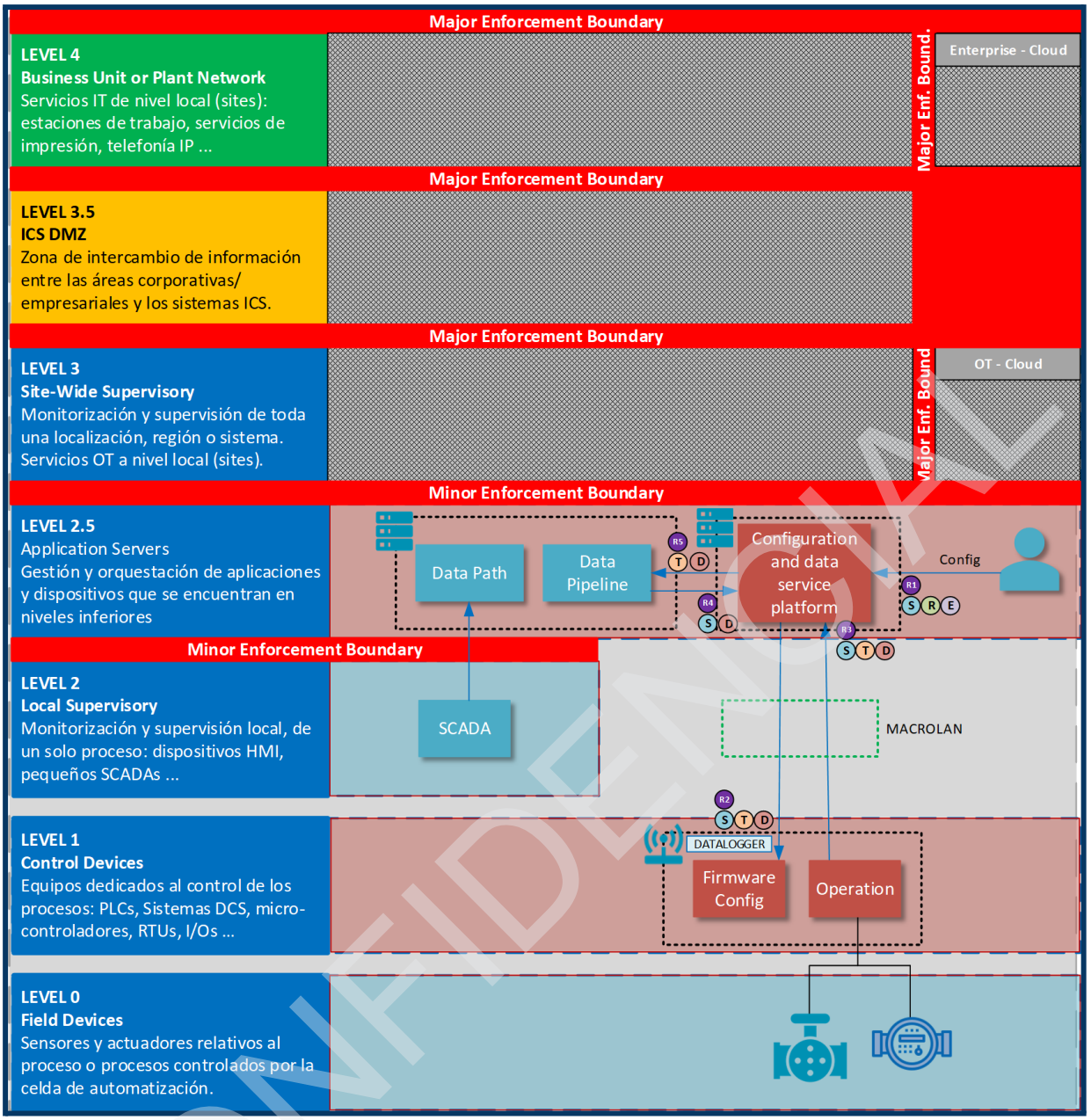
- *Spoofing* [S]: Un ciberdelincuente podría suplantar la aplicación del fabricante o reenviar las peticiones realizadas por la aplicación a los equipos con el objetivo de modificar el firmware y la configuración de los mismos. Los equipos solo deben aceptar aquellas versiones validadas por el fabricante. De lo contrario, se podrían actualizar con configuraciones inseguras.
- *Tampering* [T]: Un ciberdelincuente podría observar y modificar las tramas en la comunicación de red con la técnica del hombre en medio (*Man-in-the-Middle*) para cambiar la configuración del equipo con mala intención.
- *Denial of service* [D]: Un ciberdelincuente podría enviar una orden para apagar el equipo o sobrecargarlo de peticiones. Si eso sucediera, las actualizaciones y modificaciones legítimas de la configuración y firmware del dispositivo podrían no verse realizadas o hacerlo de una forma esperada.

R3: Este riesgo se produce en la comunicación del *datalogger* con el equipo *Edge*. Las amenazas que se podrían materializar en este canal son las siguientes:

- *Spoofing* [S]: Un dispositivo no autorizado podría suplantar al dispositivo legítimo, publicando datos y enviando información incorrecta al Edge.
- *Tampering* [T]: Un ciberdelincuente podría modificar la comunicación con el Edge a través de cambios en la trama de comunicación, publicando datos alterados al Edge
- *Denial of service* [D]: Un ciberdelincuente podría enviar una gran cantidad de tramas al Edge, apagar el proceso o atentar contra una vulnerabilidad del sistema de forma que interrumpe el servicio, provocando la pérdida de los datos que les son publicados.

Dispositivo IIoT enviando a servidor on-premise

El siguiente esquema representa la integración de un sistema IIoT enviando datos a un servidor *on-premise* que ejecuta una aplicación definida por el fabricante. La configuración del equipo también se realiza desde este servidor. Para poder tener los datos de los equipos en los sistemas de *streaming* estándar de Aigües de Barcelona, un *pipeline* situado en el mismo nivel se encarga de solicitar de forma activa estos datos. El dispositivo se encuentra integrado en un site 5 y tiene acceso a la macrolan de Aigües de Barcelona.



Esta arquitectura presenta cinco riesgos cibernéticos, en ninguno de ellos preocupa la revelación de la información ya que la confidencialidad no es una dimensión primordial en los sistemas de control industrial.

R1: Este riesgo se produce en el acceso a la aplicación web utilizada para actualizar el *firmware* o configurar los dispositivos IIoT. Las amenazas posibles son las siguientes:

- *Spoofing* [S]: Un usuario no autorizado podría acceder a la aplicación web, explotando alguna vulnerabilidad de la misma, usando técnicas de fuerza bruta u obteniendo las credenciales de un usuario legítimo. Podría realizar el alta de nuevos dispositivos, desplegar nuevas configuraciones o modificar las existentes.
- *Repudiation* [R]: Un usuario que accede a la aplicación podría realizar el alta o/y la modificación de las configuraciones. Con el objetivo de ocultar las acciones realizadas y dificultar la investigación forense podría modificar o eliminar los registros de auditoría.
- *Elevation of privileges* [E]: Un usuario que accede a la aplicación con permisos mínimos podría ampliarlos explotando alguna vulnerabilidad de la aplicación o encontrando una forma de acceder con un usuario que posea mayor rango de permisos para realizar acciones que no le están permitidas.

R2: Este riesgo se produce en la comunicación de la plataforma de configuración y servicio de datos del fabricante con los dispositivos IIoT. Las amenazas posibles son las siguientes:

- *Spoofing* [S]: Un ciberdelincuente podría suplantar la plataforma de configuración y servicio de datos del fabricante o reenviar las peticiones realizadas por esta plataforma a los equipos con el objetivo de modificar el *firmware* y la configuración de los mismos. Los equipos solo deben aceptar aquellas versiones validadas por el fabricante. De lo contrario, se podrían actualizar con configuraciones inseguras.
- *Tampering* [T]: Un ciberdelincuente podría observar y modificar las tramas en la comunicación de red con la técnica del hombre en medio (*Man-in-the-Middle*) para cambiar la configuración del equipo con mala intención.
- *Denial of service* [D]: Un ciberdelincuente podría enviar una orden para apagar el equipo o sobrecargarlo de peticiones. Si eso sucediera, las actualizaciones y modificaciones legítimas de la configuración y *firmware* del dispositivo podrían no verse realizadas o hacerlo de una forma no esperada.

R3: Este riesgo se produce en la comunicación del *datalogger* con la plataforma de configuración y servicio de datos del fabricante localizado en el centro de control. Las amenazas posibles en este canal son las siguientes:

- *Spoofing* [S]: Un dispositivo no autorizado podría suplantar al dispositivo legítimo, enviando datos incorrectos a la aplicación del fabricante.
- *Tampering* [T]: Un ciberdelincuente podría realizar cambios en la trama de comunicación del equipo con la plataforma de configuración y servicio de datos del fabricante provocando que se obtengan datos falsos, para ello podría usar la técnica del hombre en medio (*Man-in-the-Middle*).
- *Denial of service* [D]: Un ciberdelincuente podría enviar una gran cantidad de tramas a la plataforma de configuración y servicio de datos del fabricante, apagar el proceso o atentar contra una vulnerabilidad del sistema provocando su interrupción. En este caso, esta plataforma perdería todas sus funcionalidades, tanto la recogida de datos desde el dispositivo como la capacidad de modificar la configuración o el *firmware* de los mismos.

R4: Este riesgo se produce en la comunicación del *pipeline* que envía los datos del *Data Path* a la plataforma de configuración y servicio de datos del fabricante, localizada en el centro de control. Las amenazas posibles en este canal son las siguientes:

- *Spoofing* [S]: Un servicio no autorizado podría enviar una petición a la plataforma de configuración y servicio de datos del fabricante suplantando al *pipeline* legítimo para solicitar los datos emitidos por el dispositivo IIoT.
- *Denial of service* [D]: Un ciberdelincuente podría enviar una gran cantidad de tramas a la plataforma de configuración y servicio de datos del fabricante, apagar el proceso o atentar contra una vulnerabilidad del sistema provocando su interrupción. En este caso, esta plataforma perdería todas sus funcionalidades, tanto la recogida de datos desde el dispositivo como la capacidad de modificar la configuración o el *firmware* de los dispositivos IIoT.

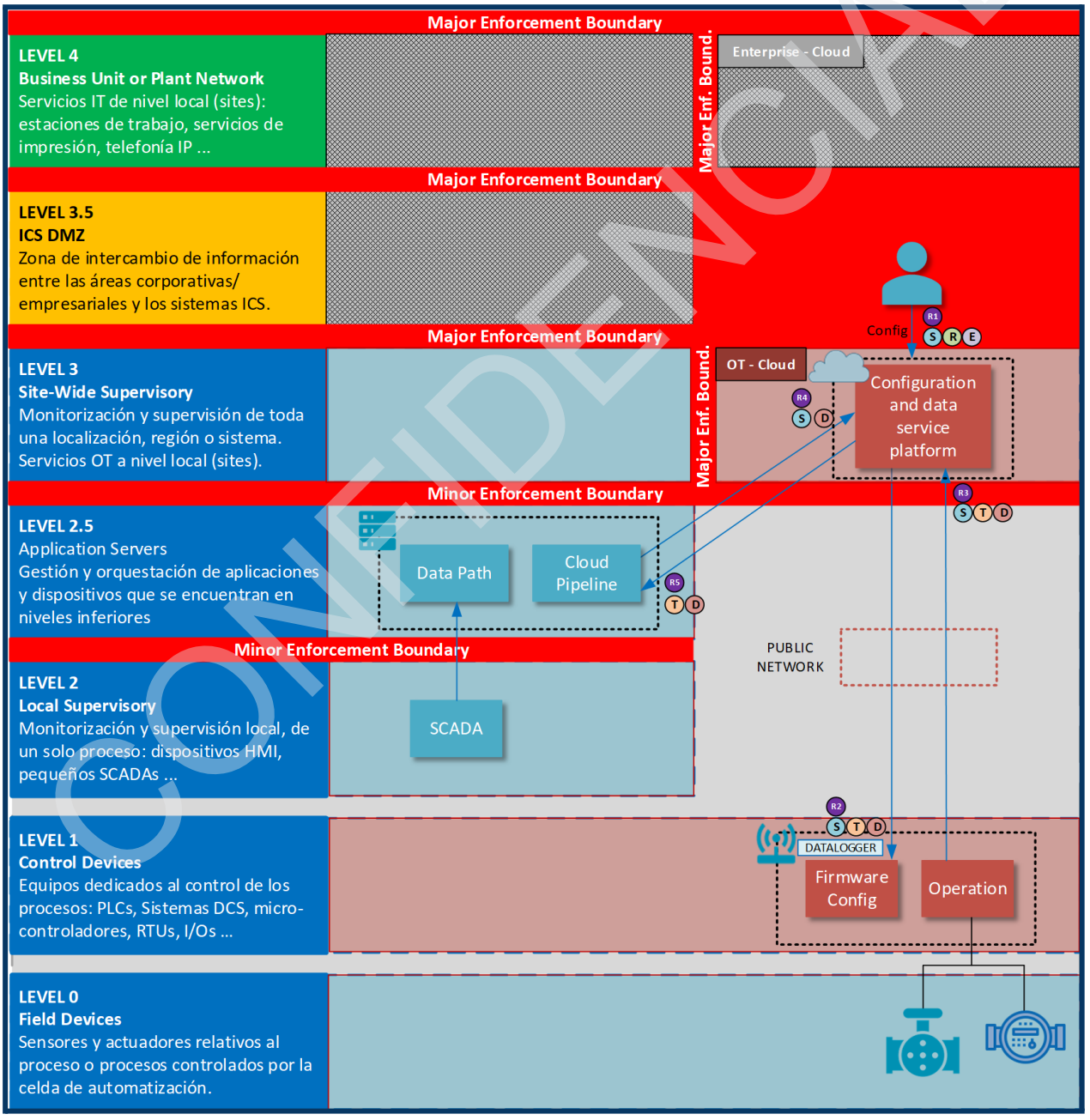
R5: Este riesgo se produce en la comunicación de la plataforma de configuración y servicio de datos del fabricante, localizada en el centro de control con el pipeline que envía los datos al *Data Path*. Las amenazas que se podrían materializar en este canal son las siguientes:

- *Tampering* [T]: Un ciberdelincuente podría realizar cambios en la trama de comunicación de la plataforma de configuración y servicio de datos del fabricante con el *pipeline* provocando que se obtengan datos falsos, para ello podría usar la técnica del hombre en medio (*Man-in-the-Middle*).

- *Denial of service* [D]: Un ciberdelincuente podría enviar una gran cantidad de tramas al *pipeline*, apagar el proceso o atentar contra una vulnerabilidad del sistema provocando su interrupción. En este caso, el *pipeline* perdería todas sus funcionalidades, tanto la recogida de datos desde la plataforma de configuración y servicio de datos como el envío de datos hacia el *Data Path*.

Dispositivo IIoT enviando a servidor en cloud

El siguiente esquema representa la integración de un sistema IIoT enviando datos a un servidor en el *Cloud* que ejecuta una aplicación definida por el fabricante. La configuración del equipo también se realiza desde este servidor. Para poder disponer de los datos de los equipos en los sistemas de *streaming* estándar de Aigües de Barcelona, un *pipeline* situado en el nivel inferior se encarga de solicitar de forma activa estos datos. El equipo que registra los datos está integrado en la instalación de tipo site 5 y tiene acceso a la red pública.



Esta arquitectura presenta cinco riesgos cibernéticos, en ninguno de ellos preocupa la revelación de la información ya que la confidencialidad no es una dimensión primordial en los sistemas de control industrial.

R1: Este riesgo se produce en el acceso a la aplicación web utilizada para actualizar el *firmware* o configurar los dispositivos IIoT. Las amenazas posibles son las siguientes:

- *Spoofing* [S]: Un usuario no autorizado podría acceder a la plataforma de configuración y servicio de datos, explotando alguna vulnerabilidad de la misma, usando técnicas de fuerza bruta u obteniendo las credenciales de un usuario legítimo. Una vez ha accedido a esta plataforma podría realizar el alta de nuevos dispositivos, desplegar nuevas configuraciones o modificar las existentes.
- *Repudiation* [R]: Un usuario que accede a la plataforma de configuración y servicio de datos podría realizar el alta o/y la modificación de las configuraciones. Con el objetivo de ocultar las acciones realizadas y dificultar la investigación forense podría modificar o eliminar los registros de auditoría, y de esta forma negar las mismas.
- *Elevation of privileges* [E]: Un usuario que accede a la aplicación con permisos mínimos podría ampliarlos explotando alguna vulnerabilidad de la plataforma de configuración y servicio de datos o encontrando una forma de acceder con un usuario que posea mayor rango de permisos para realizar acciones que no le están permitidas.

R2: Este riesgo se produce en la comunicación de la plataforma de configuración y servicio de datos del fabricante con los dispositivos IIoT. Al encontrarse estos expuestos a la red pública se incrementa la probabilidad de las amenazas que reciben con lo cual este riesgo es mayor en este sistema que el riesgo representado en la arquitectura anterior. Las amenazas que se podrían materializar en el canal son las siguientes:

- *Spoofing* [S]: Un ciberdelincuente podría suplantar la plataforma de configuración y servicio de datos del fabricante o reenviar las peticiones realizadas por esta plataforma a los equipos con el objetivo de modificar el *firmware* y la configuración de estos. Los equipos solo deben aceptar aquellas versiones validadas por el fabricante. De lo contrario, se podrían actualizar con configuraciones inseguras.
- *Tampering* [T]: Un ciberdelincuente podría observar y modificar las tramas en la comunicación de red con la técnica del hombre en medio (*Man-in-the-Middle*) para cambiar la configuración del equipo con mala intención. Esta técnica es más factible realizarla en esta arquitectura ya que el dispositivo permite el acceso desde la red pública.
- *Denial of service* [D]: Un ciberdelincuente podría enviar una orden para apagar el equipo o sobrecargarlo de peticiones. Si eso sucediera, las actualizaciones y modificaciones legítimas de la configuración y *firmware* del dispositivo podrían no verse realizadas o hacerlo de una forma esperada. Como el sistema es accesible desde la red pública el número de peticiones recibida por otros sistemas, normalmente la mayoría *bots*, incrementa exponencialmente en comparación con el tráfico que recibiría el equipo en una red privada.

R3: Este riesgo se produce en la comunicación del *datalogger* con la plataforma de configuración y servicio de datos del fabricante localizado en el Cloud. Al igual que ocurre con el equipo IIoT al estar la plataforma expuesta a la red pública, ya que se encuentra en un entorno *Cloud*, la probabilidad de que las amenazas se materialicen incrementa, con lo cual este riesgo aumenta. Las amenazas posibles en este canal son las siguientes:

- *Spoofing* [S]: Un dispositivo no autorizado podría suplantar al dispositivo legítimo, enviando datos incorrectos a la aplicación del fabricante.
- *Tampering* [T]: Un ciberdelincuente podría realizar cambios en la trama de comunicación del equipo con la plataforma de configuración y servicio de datos del fabricante

provocando que se obtengan datos falsos, para ello podría usar la técnica del hombre en medio (*Man-in-the-Middle*).
- *Denial of service* [D]: Un ciberdelincuente podría enviar una gran cantidad de tramas a la plataforma de configuración y servicio de datos del fabricante, apagar el proceso o atentar contra una vulnerabilidad del sistema provocando su interrupción. En este caso, esta plataforma perdería todas sus funcionalidades, tanto la recogida de datos desde el dispositivo como la capacidad de modificar la configuración o el *firmware* de estos.

R4: Este riesgo se produce en la comunicación del *pipeline* que envía los datos del *Data Path* a la plataforma de configuración y servicio de datos del fabricante, localizada en el *Cloud*. Las amenazas que se podrían materializar en este canal son las siguientes:

- *Spoofing* [S]: Un servicio no autorizado podría enviar una petición a la plataforma de configuración y servicio de datos del fabricante suplantando al *pipeline* legítimo para solicitar los datos emitidos por el dispositivo IIoT.
- *Denial of service* [D]: Un ciberdelincuente podría enviar una gran cantidad de tramas a la plataforma de configuración y servicio de datos del fabricante, apagar el proceso o atentar contra una vulnerabilidad del sistema provocando su interrupción. En este caso, esta plataforma perdería todas sus funcionalidades, tanto la recogida de datos desde el dispositivo como la capacidad de modificar la configuración o el *firmware* de los mismos.

R5: Este riesgo se produce en la comunicación de la plataforma de configuración y servicio de datos del fabricante localizado en el *Cloud* con el *pipeline* que envía los datos al *data path*. Las amenazas que se podrían materializar en este canal son las siguientes:

- *Tampering* [T]: Un ciberdelincuente podría realizar cambios en la trama de comunicación de la plataforma de configuración y servicio de datos del fabricante con el *pipeline* provocando que se obtengan datos falsos, para ello podría usar la técnica del hombre en medio (*Man-in-the-Middle*).
- *Denial of service* [D]: Un ciberdelincuente podría enviar una gran cantidad de tramas al *pipeline*, apagar el proceso o atentar contra una vulnerabilidad del sistema provocando su interrupción. En este caso, el *pipeline* perdería todas sus funcionalidades, tanto la recogida de datos desde la plataforma de configuración y servicio de datos como el envío de datos hacia el *data path*.

2. Requerimientos de seguridad

Los requisitos de ciberseguridad de los sistemas IIoT vienen marcados por el tipo de infraestructura en el que se integran puesto que nos fijamos en esta para definir las amenazas a las que están expuestas los activos de la red.

Cumpliendo las recomendaciones que se indican en los siguientes apartados, las cuales son requisitos marcados por la normativa ISA/IEC 62443 para tener un nivel de seguridad alto en nuestra infraestructura, se pueden minimizar e incluso eliminar en algunas ocasiones los riesgos asociados a las amenazas presentadas en los distintos tipos de sistemas con dispositivos IIoT integrados en la infraestructura de Aigües de Barcelona.

El objetivo de este apartado del informe es describir la manera en la que los productos que serán integrados en la infraestructura de Aigües de Barcelona cumplirán los requisitos que indican las diferentes certificaciones de ciberseguridad como son la Certificación Nacional Esencial de Seguridad (LINCE) o el Common Criteria (CC). De acuerdo con la legislación española es necesario que el producto ostente alguna de estas certificaciones para poder ser implementado en la infraestructura crítica de Aigües de Barcelona.

Requerimientos generales

Basándose en los tres casos de uso para integrar este tipo de solución en la arquitectura de Aigües de Barcelona a los que se les ha realizado el análisis de amenazas, se puede afirmar que el primero de ellos es el que presenta un entorno más seguro, es decir, con menor riesgo. Esto se debe únicamente a que presenta un nivel de exposición menor a las amenazas por tanto es menos probable que se materialicen. Para llevar a cabo este escenario, es necesario que el equipo IIoT disponga del protocolo MQTT.

Los componentes que conforman el sistema de control de la arquitectura de Aigües de Barcelona deben cumplir con los requisitos que se han explicado anteriormente, para ello los proveedores deben proporcionar el nivel de seguridad de capacidad (SL-C) de sus productos, de esta forma se puede comprobar si pueden ayudar al sistema a cumplir con el nivel de seguridad objetivo (SL-T). En caso de Aigües de Barcelona al tratarse de una infraestructura crítica es obligatorio, que todos los componentes que conforman el sistema de control estén certificados conforme a la Certificación Nacional Esencial de Seguridad (LINCE), acreditando la certificación básica y el Módulo de Evaluación Criptográfica (MEC), o conforme a la metodología de evaluación Common Criteria (CC). Así mismo, es necesario que el proveedor del producto que se pretende instalar en la arquitectura de Aigües de Barcelona, presente evidencias que demuestren que el producto será estable durante un largo periodo de tiempo, con este fin deberá garantizar que el producto:

- Se encuentre en funcionamiento al menos en otras cinco instalaciones más, y que esté funcionando de la forma esperada en todas ellas.
- Pueda ser instalado al menos por cinco integradores, y puedan formar a más trabajadores para ello.
- Pueda ser mantenido por integradores que se encuentren en un área cercana a la instalación de Aigües de Barcelona.
- Cuente con distribuidores locales.
- Genere y almacene registros de auditoría que permitan la monitorización del sistema completo por parte de Aigües de Barcelona.

El sistema de control industrial de Aigües de Barcelona debe contar con una plataforma de gestión que proporcione un inventario de todos los componentes instalados y de sus propiedades asociadas. Para cada componente se requiere un identificador e información sobre su versión de software, su capacidad de almacenamiento y el nivel de revisión al que se ha sometido, esta información deberá ser proporcionada por el proveedor.

Para ello, el proveedor deberá proporcionar un sistema de gestión del ciclo de vida del producto (PLM), desde la concepción hasta la retirada del mercado que garantice la liberación de actualizaciones y parches que solventen todas las vulnerabilidades detectadas en el sistema tanto en la plataforma de configuración y servicio de datos como en los dispositivos IIoT. Entre las fases del ciclo de vida se debe contemplar el intervalo en el que se emiten actualizaciones, la periodicidad de las revisiones, el procedimiento de comunicación de las actualizaciones antes de llevarla a cabo, el procedimiento desde el descubrimiento de una vulnerabilidad hasta que se solventa, etc. De esta forma evitamos la probabilidad de que una amenaza le afecte.

Aigües de Barcelona por su parte debe hacer firmar un contrato de confidencialidad de datos en la red a todos sus empleados y proveedores conocedores o con acceso a su red, a fin de evitar que compartan información sobre su sistema a través de redes sociales u otro medio que le de información a un ciberdelincuente a acceder a la red.

Requerimientos dispositivos IIoT

La plataforma de configuración y servicio de datos se conecta en los distintos casos de uso a los dispositivos IIoT para cargarles nuevas configuraciones y versiones de *firmware*. Por su parte los dispositivos IIoT pueden enviar datos a la plataforma en los casos de uso donde existe comunicación a través de la macrolan o de la red pública. Si la comunicación se realiza

completamente en la red interna los datos son subidos a un equipo *Edge*. Tanto la plataforma de configuración y servicio de datos como el dispositivo *Edge* funcionan de puente entre los dispositivos IIoT y el *data path*. Los dispositivos IIoT se encargan de recoger los datos generados por los sensores de la instalación por lo que es muy importante protegerlos para evitar anomalías en su comportamiento o la recolección de datos falsos. Basándose en la normativa ISA/IEC 62443 se diferencia entre controles recomendados y obligatorios a cumplir por el proveedor en relación con el nivel de seguridad de los dispositivos IIoT:

Control en la autenticación e identificación: El objetivo de este requisito obligatorio es que el equipo IIoT pueda asegurarse de que únicamente es accedido por la plataforma de configuración legítima. Los mecanismos requeridos para poder llevarlo a cabo son los siguientes:

- Es obligatorio que los dispositivos IIoT puedan almacenar y validar el certificado de infraestructura de clave pública (PKI) de la plataforma para garantizar la seguridad y autenticidad de ésta. Este certificado deberá estar firmado por Aigües de Barcelona y no por el proveedor del producto. Esta configuración permite que la plataforma de configuración y servicio de datos se autentique contra el dispositivo IIoT correspondiente mediante un certificado con toda su información firmado por una certificadora de confianza, un proceso que se ejecuta en estos dispositivos debe tener la capacidad de verificar la validez del certificado, de esta forma se asegura de que el proceso de la plataforma es legítimo y, por tanto, esta no se encuentra suplantada.
- Se recomienda utilizar *Trusted Platform Modules* (TPM). El equipo IIoT verifica la identidad del sistema que alberga la plataforma del propietario mediante el reconocimiento de una clave criptográfica generada por el TPM del equipo de la plataforma de configuración y servicio de datos y firmada por Aigües de Barcelona. De esta manera, se asegura que únicamente la plataforma de configuración y servicio de datos legítima albergada en el equipo ubicado en el centro de control de Aigües de Barcelona o en el Cloud se pueda comunicar con el dispositivo IIoT y se protege contra ataques de suplantación. Este certificado lo almacenaría en su propio TPM.
- Es obligatorio que, en el caso de que se quiera integrar el producto localmente, los dispositivos IIoT puedan comunicarse mediante MQTT con el bróker del dispositivo *Edge*. MQTT soporta autenticación basada en credenciales y en certificados digitales para garantizar que el dispositivo IIoT se comunica únicamente con el bróker del dispositivo *Edge* autorizado.

Control de uso: El objetivo de este requisito es restringir el uso del equipo IIoT a través de la plataforma de configuración y servicio de datos del fabricante para que evite una amplia exposición a ciberataques. Una vez que se identifica y autentica el proceso de conexión de la plataforma de configuración y servicio de datos con el dispositivo, ésta tiene permisos para actualizar el *firmware* o modificar la configuración del dispositivo siempre con código validado y durante un tiempo limitado. Los mecanismos recomendados para cumplir este requisito son los siguientes:

- Es obligatorio que los dispositivos IIoT validen las configuraciones o *firmware* antes de ser cargadas en memoria y ejecutadas.
- Es obligatorio que el dispositivo IIoT genere y almacene registros de auditoría importantes para la seguridad en las siguientes categorías: control de accesos, error de petición, eventos de la aplicación, eventos de copias de seguridad y restauración, y eventos de cambios en la configuración. Cada uno de los registros debe mostrar la fecha y la hora, el origen, la categoría, el tipo, el identificador y el resultado del evento que los ha generado. Se recomienda que el dispositivo implemente una gestión de ciclo de vida de los registros para evitar la saturación del disco.
- Es obligatorio que en el caso de que se quiera integrar el producto localmente, los dispositivos IIoT puedan comunicarse mediante MQTT con el bróker del dispositivo *Edge*. Otra de las ventajas que ofrece este protocolo es que nos permite otorgarles a los

dispositivos IIoT diferentes permisos, de esta forma se limita a que solo puedan publicar donde corresponde.

Integridad del sistema: El objetivo de este requisito es que el dispositivo IIoT mantenga su integridad física tanto si se encuentra en producción, en una parada de mantenimiento o en una zona de almacenamiento, y su integridad lógica tanto en tránsito en la red como en reposo en el dispositivo. Los mecanismos requeridos para cumplir este requisito son los siguientes:

- Cifrar la comunicación: Es un requisito obligatorio para el proveedor cifrar la comunicación realizada entre la plataforma de configuración y servicio de datos y los dispositivos IIoT. Este cifrado se debe realizar con algoritmos conocidos proporcionados por librerías de mercado mediante certificados firmados por Aigües de Barcelona y no por el proveedor del producto. Es necesario que el dispositivo IIoT utilice el certificado PKI de la plataforma de configuración y servicio de datos para cifrar la comunicación en tránsito que le envía a la plataforma.
- Es obligatorio que, en el caso de que se quiera integrar el producto localmente, los dispositivos IIoT puedan comunicarse mediante MQTT con el bróker del dispositivo *Edge* autorizado.

Disponibilidad del recurso: El objetivo de este requisito es asegurar la disponibilidad del dispositivo IIoT y prevenir situaciones de degradación o negación de sus funciones esenciales. Los mecanismos para cumplir este requisito son los siguientes:

- Gestionar las cargas de la comunicación. Es obligatorio que el dispositivo IIoT pueda limitar el número de sesiones que la plataforma de configuración y acceso de datos le mantiene activas, y que en caso de inactividad pueda cerrar las sesiones abiertas tras un tiempo configurable. También, es obligatorio que límite el número de peticiones que recibe en un mismo intervalo de tiempo. Esta medida evita que el dispositivo sea afectado por una denegación de servicios.
- Creación de copias de seguridad de la configuración y del firmware del dispositivo IIoT. La disponibilidad de copias de seguridad actualizadas es esencial para recuperar el equipo IIoT de fallos en la configuración o pérdida del *firmware*, es obligatorio para el proveedor del producto facilitar la realización de copias de seguridad y restauración de los dispositivos a través de un puerto físico, para que Aigües de Barcelona pueda recuperar la normalidad de sus procesos después de cualquier incidente en el menor tiempo posible. De este modo el tiempo de interrupción del servicio del dispositivo IIoT se reduce notablemente.
- Bastionado del dispositivo IIoT. Es obligatorio que el proveedor del producto ofrezca una guía y una interfaz para poder configurar un dispositivo IIoT de acuerdo con las directrices de seguridad y de red para protegerlo de las amenazas presentes.
- Cierre de puertos y protocolos innecesarios. Es obligatorio que el dispositivo IIoT tenga únicamente disponibles los puertos y protocolos que están en uso, tanto física como lógicamente.

Requerimientos de la plataforma de configuración y servicio de datos

La plataforma de configuración y servicio de datos se utiliza principalmente para instalar nuevas configuraciones y *firmware* en los dispositivos IIoT de la infraestructura, aunque en algunos casos de uso nos permiten recopilar los datos recogidos por estos dispositivos, y hacer de puente entre ellos y el *data path.* A fin de proteger los dispositivos IIoT de amenazas y de la pérdida de información actual en la plataforma de configuración y servicio de datos es muy importante proteger la plataforma del acceso de personas no autorizadas. Basándose en la normativa ISA/IEC 62443 se diferencia entre controles recomendados y obligatorios a cumplir por el proveedor en relación con el nivel de seguridad de la plataforma de configuración y servicio de datos:

Control en la autenticación e identificación: El objetivo de este requisito es que los sistemas que conforman la infraestructura de la nueva aplicación (plataforma de configuración y servicio de datos del fabricante, equipos IIoT, *pipeline*, dispositivos *Edge*, y los sistemas que lo albergan independientemente de si se encuentran *On Premise* o en *Cloud*) identifiquen y autentiquen correctamente a todos los usuarios (humanos o procesos de software) que pidan acceder a ellos antes de iniciar la comunicación. Los mecanismos requeridos para cumplir este requisito son los siguientes:

- Es obligatorio que todos los usuarios humanos utilicen contraseñas robustas y que a todas las cuentas pertenecientes a procesos se les asignen tokens robustos, que presenten diversidad en el tipo de caracteres y una longitud mínima.
- Es obligatorio ofuscar la contraseña mientras que el usuario humano la escribe para registrarse o iniciar sesión, y omitir cualquier información que un usuario pueda asociar a la existencia de una cuenta.
- Es recomendado habilitar un doble factor de autenticación para los usuarios humanos que inicien sesión en el portal web, por ejemplo, utilizar una contraseña y una clave obtenida mediante SMS o al permitir sincronizar una aplicación de autenticación, o utilizar un factor biométrico.
- Es obligatorio que permita la modificación del autenticador usado (contraseñas, tokens, claves simétricas o claves privadas). Si la cuenta se crea por defecto, el propietario deberá generar una nueva autenticación para acceder en el primer inicio de sesión. Los usuarios de la plataforma se deben ver obligados a modificar su autenticador cada cierto tiempo, por ejemplo, una vez al año, en el caso de no usar un doble factor de autenticación. El nuevo secreto no debe haber sido usado en ocasiones anteriores por el mismo usuario. De esta forma se reduce la probabilidad de que consigan el acceso a la plataforma mediante fuerza bruta.
- Es obligatorio que se permita la gestión de cuentas desde el portal web a un usuario administrador, que poseerá permisos para añadir, eliminar, habilitar, deshabilitar y cambiar la configuración de otras cuentas, como puede ser habilitar o deshabilitar factores de autenticación, o gestionar los permisos o roles.
- Es obligatorio que la plataforma de configuración y servicio de datos permita la configuración de número de intentos límites para iniciar sesión con una cuenta, la aplicación web debe bloquear durante un periodo corto de tiempo la cuenta.
- Es obligatorio que la plataforma de configuración y servicio de datos permita instalar un certificado de infraestructura de clave pública (PKI) para garantizar la seguridad y autenticidad de la conexión entre la aplicación y los distintos procesos que se comuniquen con ella, como son el navegador del usuario, el proceso del *pipeline*, o el proceso de los equipos IIoT. Este certificado deberá estar firmado por Aigües de Barcelona y no por el proveedor de la aplicación. Esta configuración permite que la plataforma de configuración y servicio de datos se autentique contra el dispositivo IIoT correspondiente mediante un certificado con toda su información firmado por una certificadora de confianza, un proceso que se ejecuta en estos dispositivos debe tener la capacidad de verificar la validez del certificado, de esta forma se asegura de que la página no está suplantada y la comunicación realizada sea cifrada.
- Es obligatorio que el acceso a la plataforma de configuración y servicio de datos muestre un mensaje de bienvenida que indique que se está accediendo a un sistema crítico y las leyes a las que se enfrenta una persona que haga un uso no permitido de la aplicación.

Control de uso: El objetivo de este requisito es restringir el uso de la plataforma de configuración y servicio de datos a los permisos que posee cada usuario (humanos o procesos de software). Una vez que el usuario es identificado y autenticado, la plataforma de configuración y servicio de datos debe restringir las acciones permitidas que cada usuario puede realizar de acuerdo con sus privilegios. Los mecanismos requeridos para cumplir este requisito son los siguientes:

- Se recomienda que permita la configuración de grupo de usuarios o roles.
- Es obligatorio que permita la asignación de permisos a usuarios, pudiéndolos asignar tanto a un único usuario como a todos los usuarios pertenecientes a un grupo, en caso de que se puedan configurar grupos o roles. Los permisos otorgados a cualquier cuenta que tenga acceso a la aplicación deberán ser mínimas para desarrollar las tareas que le han sido encomendadas adecuadamente. En el caso de que una cuenta ostente más de un rol, se le ampliarían sus permisos para realizar las acciones encomendadas gracias a esta funcionalidad.
- Es obligatorio que la plataforma de configuración y servicio de datos bloquee la sesión web de forma automática después de un tiempo de inactividad configurable por el administrador, permaneciendo así hasta que otro usuario humano restablezca el acceso. Esta medida solo se aplica a sesiones abiertas en el portal web, previniendo que otros usuarios no autorizados accedan a la aplicación.
- Es obligatorio que la plataforma de configuración y servicio de datos limite el número de sesiones concurrentes que puede mantener abierta un mismo usuario, de esta forma se evitan conflictos entre las acciones realizadas. Esta tasa límite de sesiones se debe generalizar para evitar ataques de denegación de servicios en el caso de recepción masiva de solicitudes de autorización.
- Es obligatorio que la plataforma de configuración y servicio de datos compruebe las configuraciones o *firmware* antes de ser enviadas a los equipos IIoT. La aplicación se debe encargar de prevenir la transferencia del código hasta que no compruebe correctamente su proveniencia, y lo valide. La aplicación debe almacenar un historial del código enviado a los dispositivos.
- Es obligatorio que la plataforma de configuración y servicio de datos se comunique por OPC UA para servir los datos al *pipeline* en el caso de que la plataforma no se encuentre en un entorno *Cloud,* o permitir la utilización de API REST en caso de que se encuentre en un entorno *Cloud.*
- Es obligatorio que la plataforma de configuración y servicio de datos genere y almacene en el equipo registros de auditoría importantes para la seguridad en las siguientes categorías: control de accesos, error de petición, eventos de la aplicación, eventos de copias de seguridad y restauración, y eventos de cambios en la configuración. Cada uno de los registros debe mostrar la fecha y la hora, el origen, la categoría, el tipo, el identificador y el resultado del evento que los ha generado. Estos registros deben incluir todas aquellas acciones permitidas en la aplicación, como la realización de un cambio de la configuración o la actualización del *firmware* de un dispositivo IIoT.

Disponibilidad del recurso: El objetivo de este requisito es asegurar la disponibilidad de la plataforma del fabricante y prevenir situaciones de degradación o negación de la recepción de datos. Los mecanismos requeridos para cumplir este requisito son los siguientes:

- Gestionar las cargas de la comunicación. Es obligatorio que la plataforma del fabricante pueda limitar el número de sesiones que mantiene abiertas y limitar el número de peticiones que recibe. Así mismo, debe cerrar automáticamente aquellas sesiones inactivas que mantiene abiertas contra los dispositivos IIoT tras un tiempo configurable por un usuario administrador. Esta medida evita que el dispositivo sea afectado por una denegación de servicios.
- Creación de copias de seguridad de las configuraciones y la información de usuarios y dispositivos albergada en la plataforma. La disponibilidad de copias de seguridad actualizadas es esencial para recuperar la plataforma en caso de ser alcanzada por un ataque que provoque la negación de sus servicios, es obligatorio que la plataforma de configuración y servicio de datos facilite la realización y restauración de las copias de seguridad de la información que almacena, para recuperar la normalidad de sus procesos después de cualquier incidente en el menor tiempo posible. De este modo el tiempo de interrupción del servicio de la plataforma se reduce notablemente.
- Bastionado del servidor que alberga la plataforma de configuración y servicio de datos. Es obligatorio que el proveedor del producto configure el equipo donde alberga su

plataforma de configuración y servicio de datos siguiendo la guía del fabricante de acuerdo a unas buenas prácticas de seguridad para reducir la posibilidad de ataque, si la plataforma se encuentra en un entorno *Cloud*, se deberán aplicar del mismo modo las recomendaciones indicadas por la empresa propietaria del *Cloud* para proteger a la plataforma.

- Cierre de puertos y protocolos innecesarios. Es obligatorio que el equipo o entorno que alberga la plataforma de configuración y servicio de datos debe tener únicamente disponibles los puertos y protocolos que están en uso, bien sean físicos o lógicos.
- Anular manualmente la sesión de conexión a un dispositivo. Es obligatorio que la plataforma de configuración y servicio de datos permita a un usuario administrador anular la sesión del usuario actual conectado al dispositivo de forma manual en caso de emergencia durante un tiempo configurable o tras una secuencia de eventos.
- Uso de *Over-the-air* (OTA). Es obligatorio que la plataforma de configuración y servicio de datos permita la actualización de todos los dispositivos IIoT mediante tecnología OTA de forma masiva.

Por último, se recomienda que en el caso en que la plataforma de configuración y servicio de datos deba ejecutarse en el Cloud, este pertenezca a Aigües de Barcelona y no al proveedor de la aplicación. Si este requisito no puede cumplirse, es un requisito obligatorio que el proveedor ostente la certificación de la normativa ISO 27001, para que pueda prevenirse de los riesgos ante una amenaza, conozca la forma de mitigarla, para que Aigües de Barcelona no se encuentre afectado.

3. Tablas resumen

Tabla resumen de requisitos generales por parte del proveedor para el sistema

N	REQUISITO	OBLIGATORIO	RECOMENDADO
1	Procedimiento *Product Life Management* (PLM)	X	
2	Certificación LINCE o CC	X	
3	Garantía del correcto funcionamiento de la aplicación en, al menos, otras cinco instalaciones	X	
4	Garantía de que al menos existen cinco personas capacitadas para su integración	X	
5	Garantía de distribuidores locales	X	
6	Garantía de técnicos de mantenimiento cerca de la instalación	X	
7	Firma del contrato de confidencialidad	X	
8	Certificación ISO 27001 si el Cloud pertenece al proveedor de la solución	X	

Tabla resumen de requisitos por parte del proveedor para los dispositivos IoT

N	REQUISITO	OBLIGATORIO	RECOMENDADO
1	Límite del número de sesiones que puede mantener abierta	X	
2	Cierre automático de sesiones inactivas	X	
3	Comprobación de las configuraciones o firmware antes de ser cargadas en memoria	X	
4	Cifrado de la información en tránsito mediante el uso de certificado de infraestructura de clave pública (PKI) de la plataforma	X	
5	Creación de registros de auditoría	X	
6	Gestión del almacenamiento de registros para evitar la saturación del dispositivo		X
7	Límite del número de peticiones que puede recibir en un mismo intervalo de tiempo	X	
8	Realización de copias de seguridad de las configuraciones y *firmware* aplicados desde el mismo dispositivo IoT	X	
9	Opción para la recuperación del sistema mediante la copia de seguridad extraída	X	
10	Cierre de puertos y protocolos innecesarios de dispositivos IoT	X	
11	Guía de bastionado para los dispositivos IoT	X	
12	Uso de *Trusted Platform Modules* (TPM)		X
13	Uso del protocolo MQTT si es integrado localmente	X	

Tabla resumen de requisitos por parte del proveedor para la plataforma de configuración y servicio de datos

N	REQUISITO	OBLIGATORIO	RECOMENDADO
1	Configuración de grupo de usuarios o roles		X
2	Segregación de permisos para realizar las diferentes acciones permitidas en la aplicación	X	
3	Opción para asignar permisos a usuarios o roles	X	
4	Bloqueo de la sesión web después de un periodo de inactividad	X	
5	Límite del número de sesiones concurrentes que puede mantener abierta un mismo usuario	X	
6	Validación de las configuraciones o firmware antes de ser enviadas al dispositivo IIoT	X	
7	Uso de secretos robustos (contraseñas, tokens, firmas, etc.)	X	
8	Ocultación de contraseña mientras el usuario la escribe	X	
9	Ocultación de información específica sobre el acceso al usuario	X	
10	Opción de acceso mediante 2FA		X
11	Modificación de secreto	X	
12	Gestión de cuentas desde el panel de administrador	X	
13	Número de intentos límites para acceder mediante tiempo de bloqueo		X
14	Cifrado de la información en tránsito mediante el uso de certificado de infraestructura de clave pública (PKI)	X	
15	Mensaje de bienvenida informando sobre la legislación aplicable	X	
16	Creación de registros de auditoría	X	
17	Gestión del almacenamiento de registros para evitar la saturación del sistema		X
18	Límite del número de peticiones que puede recibir en un mismo intervalo de tiempo	X	
19	Opción de realización de copias de seguridad de las configuraciones y *firmware* aplicados en los dispositivos IIoT	X	
20	Opción de realización de copias de seguridad del sistema de usuarios y autorizaciones	X	
21	Opción para cargar una copia de seguridad desde la plataforma para la recuperación del sistema	X	
22	Cierre de puertos y protocolos innecesarios de la plataforma	X	
23	Bastionado del equipo donde se encuentra instalada la plataforma	X	
24	Uso de *Trusted Platform Modules* (TPM) en el equipo donde se encuentra instalada la plataforma		X
25	Opción a un usuario administrador para anular la sesión de un usuario conectado		X
26	Cierre de las comunicaciones inactivas automáticamente		X
27	Actualización masiva mediante tecnología *Over-the-air* (OTA)	X	
28	Comunicación mediante OPC UA o API REST con el *pipeline*	X	
29	Instalación local		X

Anexo 4: Datos a enviar a sistema IIoT (Hojas de cálculo de Google)

Ubicación	Referencia	Marca	SUM de Cantidad
PT-01-00-PR-145	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
PT-01-00-PR-21	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
PT-01-02-PR-01	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
PT-03-00-PR-10	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
			8
EBAR AVANTPORT NORD (Salida bombeo)	CAUDAL_LASER	Teledyne ISCO	1
EBAR AVANTPORT SUD (Salida bombeo)	CAUDAL_MAG_PN10	Endress	6
EBAR CORNELLÀ PT-03-00-PR-04 (Salida bombeo)	CAUDAL_LASER	Teledyne ISCO	1
EBAR PRAT PT-02-00-PR-02 (Salida bombeo)	CAUDAL_LASER	Teledyne ISCO	1
EBAR SANT BOI (Salida bombeo)	CAUDAL_LASER	Teledyne ISCO	1
EBAR ZONA FRANCA PT-04-00-PR-76B (Salida bombeo)	CAUDAL_LASER	Teledyne ISCO	1
			11
EQ CASTELLBISBAL	HACH_SON_COND	HACH	1
	HACH_SON_PH	HACH	1
	HACH_SON_REDOX	HACH	1
	HACH_SON_TUSS	HACH	1
			4
PT-04-00-PR-29	DATA_COND	SOFREL	1
PT-04-00-PR-44	DATA_COND	SOFREL	1
PT-04-00-SB-59a	DATA_COND	SOFREL	1
			3
EBAR CAN GUITART	MULTISONDA1	Mejoras energéticas	1
EBAR CAN PALET	MULTISONDA1	Mejoras energéticas	1
EBAR RAFAMANS	MULTISONDA2	XYLEM YSI	1
EBAR SANT BARTOMEU	MULTISONDA1	Mejoras energéticas	1
EBAR VALLPINEDA 2	MULTISONDA1	Mejoras energéticas	1
SF-02-03-CB_SB-66 Can Cases	DATA_COND	SOFREL	1
	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
SF-03-06-PR-77 Riera cervelló	DATA_COND	SOFREL	1
	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
SF-03-08-PR-50 Riera Torrelles	DATA_COND	SOFREL	1
	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
			14
Ca n'Armengol	PLUVIOMETRO	Lambrecht	1
Can Güell	PLUVIOMETRO	Lambrecht	1
			2
EDAR EL PRAT (Entrada lado Barcelona)	CAUDAL_LASER	Teledyne ISCO	1

Ubicación	Referencia	Marca	SUM de Cantidad
EDAR EL PRAT (Entrada lado Prat)	CAUDAL_LASER	Teledyne ISCO	1
EDAR GAVÀ (Entrada)	CAUDAL_LASER	Teledyne ISCO	1
EDAR SANT FELIU (Entrada)	CAUDAL_LASER_SUM	Teledyne ISCO	1
			4
EDAR EL PRAT (Entrada lado Barcelona)	HACH_AN_AMONIO_1K	HACH	1
	HACH_SON_COND	HACH	1
	HACH_SON_ODIS	HACH	1
	HACH_SON_PH	HACH	1
	HACH_SON_REDOX	HACH	1
	HACH_SON_TUSS	HACH	1
EDAR EL PRAT (Entrada lado Prat)	HACH_AN_AMONIO_1K	HACH	1
	HACH_SON_COND	HACH	1
	HACH_SON_ODIS	HACH	1
	HACH_SON_PH	HACH	1
	HACH_SON_REDOX	HACH	1
	HACH_SON_TUSS	HACH	1
EDAR GAVÀ (Entrada)	HACH_AN_AMONIO_1K	HACH	1
	HACH_SON_ODIS	HACH	1
	HACH_SON_REDOX	HACH	1
	HACH_SON_TUSS	HACH	1
EDAR SANT FELIU (Entrada)	HACH_AN_AMONIO_1K	HACH	1
	HACH_SON_COND	HACH	1
	HACH_SON_ODIS	HACH	1
	HACH_SON_REDOX	HACH	1
	HACH_SON_TUSS	HACH	1
			21
EBAR AVANTPORT SUD	1408-TS3A-ENT	Rockwell	6
EDAR GAVÀ	1408-TS3A-ENT	Rockwell	30
EDAR PRAT	1408-TS3A-ENT	Rockwell	81
EDAR SANT FELIU	1408-TS3A-ENT	Rockwell	16
			133
BS-02-00-PR_SB-05	DATA_LT-US	SOFREL	1
BS-02-00-PR_SB-168	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
BS-03-00-PR_CN_SB-20	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
BS-03-00-PR_SB-41	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
Equipo Móvil	DATA_LT-US	SOFREL	2
	DATALOGGER	SOFREL	2
GV-02-00-PR_SB-20	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
GV-03-06-PR_SB-10	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1

Ubicación	Referencia	Marca	SUM de Cantidad
GV-03-02-PR_SB-3.09	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
GV-03-04-CB_SB-37a	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
MN-04-01-PR_SB-02	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
MN-04-03-CN_SB-01	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
PT-02-08-SB	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
PT-01-00-CB_SB-70	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
PT-01-08-PR_SB-02	DATA_LT-US	SOFREL	2
	DATALOGGER	SOFREL	1
PT-01-08-PR_SB-22	DATALOGGER	SOFREL	1
PT-01-08-PR_SB-28	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
PT-01-09-PR_SB-04	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
PT-02-04-PR_SB-13	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
PT-03-01-CB_CN_SB-02	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
PT-03-01-PR_SB-41	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
PT-03-03-PR_SB-17	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
PT-03-03-PRp_SB-13	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
PT-03-05-PR_SB-06	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
PT-04-00-PR_SB-115	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
SF-03-16-PR_SB-29	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
SF-03-16-PR-CN-SB-04	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
SF-01-00-CB_SB-63	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
SF-01-00-SI_SB-01	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
SF-02-03-CB_SB-66	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
SF-02-07-CN_SB-05.1	DATA_LT-US	SOFREL	1

Ubicación	Referencia	Marca	SUM de Cantidad
	DATALOGGER	SOFREL	1
SF-03-00-SI_SB-10	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
SF-03-07-PR_CN_SB-01	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
SF-03-08-PR_SB-04	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
SF-03-13-PR_SB-06	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
SF-04-00-PR_SB-06	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
SF-04-00-PR_SB-54	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
SF-04-02-PR_SB-04	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
SF-04-08-PR_SB-06	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
SF-05-00-CB_SB-07	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
SF-05-00-PR_SB-01	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
SF-05-00-PR_SB-39	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
			83
BS-02-01-EB_SB-06 (Alivio)	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
BS-02-02-DE_SB-03.2 (Alivio)	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
GV-01-00-SB-EEBB-Interceptor Castelldefels (Alivio)	CAUDAL_MAG_PN10	Endress	1
GV-02-00-PR_SB-20 (Alivio)	DATA_LT-US	SOFREL	1
	DATALOGGER	SOFREL	1
PT-01-01-PR_SB-02 (Alivio EBAR Sant Boi)	CAUDAL_LASER	Teledyne ISCO	1
PT-02-00-PR_SB-04 (Alivio EBAR Prat)	CAUDAL_LASER	Teledyne ISCO	1
			9
EBAR BAC DE RODA	HACH_SON_COND	HACH	1
	HACH_SON_ODIS	HACH	1
	HACH_SON_PH	HACH	1
	HACH_SON_TUSS	HACH	1
EBAR CORNELLÀ	HACH_SON_COND	HACH	1
	HACH_SON_ODIS	HACH	1
	HACH_SON_PH	HACH	1
	HACH_SON_TUSS	HACH	1
EBAR INTERCEPTOR DE CASTELLDEFELS	HACH_SON_COND	HACH	1
	HACH_SON_ODIS	HACH	1

Ubicación	Referencia	Marca	SUM de Cantidad
	HACH_SON_PH	HACH	1
	HACH_SON_TUSS	HACH	1
EBAR SANT ADRIÀ	HACH_SON_COND	HACH	1
	HACH_SON_ODIS	HACH	1
	HACH_SON_PH	HACH	1
	HACH_SON_TUSS	HACH	1
			16
EDAR PRAT (Vertido - lado Barcelona)	CAUDAL_LASER	Teledyne ISCO	1
EDAR PRAT (Vertido - lado Prat)	CAUDAL_LASER	Teledyne ISCO	1
			2
EDAR EL PRAT (Salida secundario lado Barcelona)	HACH_SON_COND	HACH	1
	HACH_SON_DQO	HACH	1
	HACH_SON_PH	HACH	1
EDAR EL PRAT (Salida secundario lado Prat)	HACH_NITRAX	HACH	1
	HACH_SON_COND	HACH	1
	HACH_SON_DQO	HACH	1
	HACH_SON_PH	HACH	1
	HACH_SON_TUSS	HACH	1
EDAR GAVÀ (Salida Zona IFAS)	HACH_SON_DQO	HACH	1
	HACH_SON_PH	HACH	1
EDAR GAVÀ (Salida Zona MBR)	HACH_SON_DQO	HACH	1
	HACH_SON_PH	HACH	1
EDAR SANT FELIU (Salida secundario)	HACH_SON_COND	HACH	1
	HACH_SON_DQO	HACH	1
	HACH_SON_PH	HACH	1
			15
EDAR GAVÀ (Emisario - Alivio Pluviales)	CAUDAL_LASER	Teledyne ISCO	1
EDAR MONTCADA (Alivio entrada Biológico)	NIVELRADAR	VEGA	1
EDAR PRAT (Alivio Bombeo Intermedio)	NIVELRADAR	VEGA	1
EDAR PRAT (Alivio salida desarenadores - lado Barcelona)	NIVELRADAR	VEGA	1
EDAR PRAT (Alivio salida desarenadores - lado Prat)	NIVELRADAR	VEGA	1
			5
			330

Nuevo	Tipo de equipo	Tipo de sede	Nombre sede	Nombre equipo /	Variable /	Numero	Nombre PLC/Datalogger	Frecuencia	Frecuencia envio	Volumen neto dato	Origen del dato/calculo	Ubicación	Capacidad	Total
Sí	Caudalimetro	RED COLECTORES	PT-01-00-PR-145	PT-01-00-PR-145	Nivel	1	PT-01-00-PR-145	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-01-00-PR-145	PT-01-00-PR-145	Velocidad superficial	1	PT-01-00-PR-145	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-01-00-PR-145	PT-01-00-PR-145	Caudal	1	PT-01-00-PR-145	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-01-02-PR01	PT-01-02-PR01	Nivel	1	PT-01-02-PR01	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-01-02-PR01	PT-01-02-PR01	Velocidad superficial	1	PT-01-02-PR01	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-01-02-PR01	PT-01-02-PR01	Caudal	1	PT-01-02-PR01	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PR-03-00-PR-10	PR-03-00-PR-10	Nivel	1	PR-03-00-PR-10	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PR-03-00-PR-10	PR-03-00-PR-10	Velocidad superficial	1	PR-03-00-PR-10	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PR-03-00-PR-10	PR-03-00-PR-10	Caudal	1	PR-03-00-PR-10	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-01-00-PR-21	PT-01-00-PR-21	Nivel	1	PT-01-00-PR-21	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-01-00-PR-21	PT-01-00-PR-21	Velocidad superficial	1	PT-01-00-PR-21	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-01-00-PR-21	PT-01-00-PR-21	Caudal	1	PT-01-00-PR-21	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	12
Sí	Caudalimetro Laser	EBAR	EBAR Prat	Bombeo	Caudal bombeado	1	EBAR Prat	5 min	5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro Laser	EBAR	EBAR Prat	Bombeo	Velocidad	1	EBAR Prat	5 min	5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro Laser	EBAR	EBAR Prat	Bombeo	Nivell	1	EBAR Prat	5 min	5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	EBAR	EBAR Avantpor Sud	Bomba 1	Caudal bombeado	1	EBAR Avantpor Sud	5 min	5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	EBAR	EBAR Avantpor Sud	Bomba 2	Caudal bombeado	1	EBAR Avantpor Sud	5 min	5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	EBAR	EBAR Avantpor Sud	Bomba 3	Caudal bombeado	1	EBAR Avantpor Sud	5 min	5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	EBAR	EBAR Avantpor Sud	Bomba 4	Caudal bombeado	1	EBAR Avantpor Sud	5 min	5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	EBAR	EBAR Avantpor Sud	Bomba 5	Caudal bombeado	1	EBAR Avantpor Sud	5 min	5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	EBAR	EBAR Avantpor Sud	Bomba 6	Caudal bombeado	1	EBAR Avantpor Sud	5 min	5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro Laser	EBAR	EBAR Cornellà	Bombeo	Caudal bombeado	1	EBAR Cornellà	5 min	5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro Laser	EBAR	EBAR Cornellà	Bombeo	Velocidad	1	EBAR Cornellà	5 min	5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro Laser	EBAR	EBAR Cornellà	Bombeo	Nivell	1	EBAR Cornellà	5 min	5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro Laser	EBAR	EBAR Zona Franca	Bombeo	Caudal bombeado	1	EBAR Zona Franca	5 min	5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro Laser	EBAR	EBAR Zona Franca	Bombeo	Velocidad	1	EBAR Zona Franca	5 min	5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro Laser	EBAR	EBAR Zona Franca	Bombeo	Nivell	1	EBAR Zona Franca	5 min	5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro Laser	EBAR	EBAR Avantport Nord	Bombeo	Caudal bombeado	1	EBAR Avantport Nord	5 min	5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro Laser	EBAR	EBAR Avantport Nord	Bombeo	Velocidad	1	EBAR Avantport Nord	5 min	5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro Laser	EBAR	EBAR Avantport Nord	Bombeo	Nivell	1	EBAR Avantport Nord	5 min	5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro Laser	EBAR	EBAR Sant Boi	Bombeo	Caudal bombeado	1	EBAR Sant Boi	5 min	5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro Laser	EBAR	EBAR Sant Boi	Bombeo	Velocidad	1	EBAR Sant Boi	5 min	5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro Laser	EBAR	EBAR Sant Boi	Bombeo	Nivell	1	EBAR Sant Boi	5 min	5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
No	Estado EBARs existentes	EBAR	EBAR Ginebra	Bombeo	Estado bombas, averias, caudal bombeado, etc...	30	EBAR Ginebra	5 min	5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
No	Estado EBARs existentes	EBAR	EBAR Sant Adrià	Bombeo	Estado bombas, averias, caudal bombeado, etc...	30	EBAR Sant Adrià	5 min	5 min	Decimal	PLC Pooling EDAR Besos	EDAR Besos	72h	
No	Estado EBARs existentes	EBAR	EBAR Procolor	Bombeo	Estado bombas, averias, caudal bombeado, etc...	30	EBAR Procolor	5 min	5 min	Decimal	PLC Pooling EDAR Besos	EDAR Besos	72h	
No	Estado EBARs existentes	EBAR	EBAR Bac de Roda	Bombeo	Estado bombas, averias, caudal bombeado, etc...	30	EBAR Bac de Roda	5 min	5 min	Decimal	PLC Pooling EDAR Besos	EDAR Besos	72h	
No	Estado EBARs existentes	EBAR	EBAR Badalona	Bombeo	Estado bombas, averias, caudal bombeado, etc...	30	EBAR Badalona	5 min	5 min	Decimal	PLC Pooling EDAR Besos	EDAR Besos	72h	
No	Estado EBARs existentes	EBAR	EBAR Montgat 2	Bombeo	Estado bombas, averias, caudal bombeado, etc...	30	EBAR Montgat 2	5 min	5 min	Decimal	PLC Pooling EDAR Besos	EDAR Besos	72h	
No	Estado EBARs existentes	EBAR	EBAR Montgat 3	Bombeo	Estado bombas, averias, caudal bombeado, etc...	30	EBAR Montgat 3	5 min	5 min	Decimal	PLC Pooling EDAR Besos	EDAR Besos	72h	
No	Estado EBARs existentes	EBAR	EBAR Montgat 1	Bombeo	Estado bombas, averias, caudal bombeado, etc...	30	EBAR Montgat 1	5 min	5 min	Decimal	PLC Pooling EDAR Besos	EDAR Besos	72h	
No	Estado EBARs existentes	EBAR	EBAR Castelldefels 3	Bombeo	Estado bombas, averias, caudal bombeado, etc...	30	EBAR Castelldefels 3	5 min	5 min	Decimal	PLC Pooling EDAR Gavà	EDAR Gavá	72h	
No	Estado EBARs existentes	EBAR	EBAR Castelldefels 1	Bombeo	Estado bombas, averias, caudal bombeado, etc...	30	EBAR Castelldefels 1	5 min	5 min	Decimal	PLC Pooling EDAR Gavà	EDAR Gavá	72h	
No	Estado EBARs existentes	EBAR	EBAR Castelldefels 2	Bombeo	Estado bombas, averias, caudal bombeado, etc...	30	EBAR Castelldefels 2	5 min	5 min	Decimal	PLC Pooling EDAR Gavà	EDAR Gavá	72h	
No	Estado EBARs existentes	EBAR	EBAR Gavà 1	Bombeo	Estado bombas, averias, caudal bombeado, etc...	30	EBAR Gavà 1	5 min	5 min	Decimal	PLC Pooling EDAR Gavà	EDAR Gavá	72h	
No	Estado EBARs existentes	EBAR	EBAR Gavà 2	Bombeo	Estado bombas, averias, caudal bombeado, etc...	30	EBAR Gavà 2	5 min	5 min	Decimal	PLC Pooling EDAR Gavà	EDAR Gavá	72h	
No	Estado EBARs existentes	EBAR	EBAR Castelldefels 4	Bombeo	Estado bombas, averias, caudal bombeado, etc...	30	EBAR Castelldefels 4	5 min	5 min	Decimal	PLC Pooling EDAR Gavà	EDAR Gavá	72h	
No	Estado EBARs existentes	EBAR	EBAR Sant Boi Viladecans	Bombeo	Estado bombas, averias, caudal bombeado, etc...	30	EBAR Sant Boi Viladecans	5 min	5 min	Decimal	PLC Pooling EDAR Gavà	EDAR Gavá	72h	
No	Estado EBARs existentes	EBAR	EBAR Can Espinós	Bombeo	Estado bombas, averias, caudal bombeado, etc...	30	EBAR Can Espinós	5 min	5 min	Decimal	PLC Pooling EDAR Gavà	EDAR Gavá	72h	
No	Estado EBARs existentes	EBAR	EBAR Interceptor Castelldefels	Bombeo	Estado bombas, averias, caudal bombeado, etc...	30	EBAR Interceptor Castelldefels	5 min	5 min	Decimal	PLC Pooling EDAR Gavà	EDAR Gavá	72h	
No	Estado EBARs existentes	EBAR	EBAR Begues Park	Bombeo	Estado bombas, averias, caudal bombeado, etc...	30	EBAR Begues Park	5 min	5 min	Decimal	PLC Pooling EDAR Gavà	EDAR Gavá	72h	
No	Estado EBARs existentes	EBAR	EBAR Prat	Bombeo	Estado bombas, averias, caudal bombeado, etc...	30	EBAR Prat	5 min	5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
No	Estado EBARs existentes	EBAR	EBAR Cornellà	Bombeo	Estado bombas, averias, caudal bombeado, etc...	30	EBAR Cornellà	5 min	5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
No	Estado EBARs existentes	EBAR	EBAR Zona Franca	Bombeo	Estado bombas, averias, caudal bombeado, etc...	30	EBAR Zona Franca	5 min	5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
No	Estado EBARs existentes	EBAR	EBAR Puerto Sur	Bombeo	Estado bombas, averias, caudal bombeado, etc...	30	EBAR Puerto Sur	5 min	5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
No	Estado EBARs existentes	EBAR	EBAR Sant Boi	Bombeo	Estado bombas, averias, caudal bombeado, etc...	30	EBAR Sant Boi	5 min	5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
No	Estado EBARs existentes	EBAR	EBAR Puerto Norte	Bombeo	Estado bombas, averias, caudal bombeado, etc...	30	EBAR Puerto Norte	5 min	5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
No	Estado EBARs existentes	EBAR	EBAR Can Armengol	Bombeo	Estado bombas, averias, caudal bombeado, etc...	30	EBAR Can Armengol	5 min	5 min	Decimal	PLC Pooling EDAR Sant Feliu	EDAR Sant Feliu	72h	
No	Estado EBARs existentes	EBAR	EBAR Sant Bartomeu	Bombeo	Estado bombas, averias, caudal bombeado, etc...	30	EBAR Sant Bartomeu	5 min	5 min	Decimal	PLC Pooling EDAR Sant Feliu	EDAR Sant Feliu	72h	
No	Estado EBARs existentes	EBAR	EBAR Can Palet	Bombeo	Estado bombas, averias, caudal bombeado, etc...	30	EBAR Can Palet	5 min	5 min	Decimal	PLC Pooling EDAR Sant Feliu	EDAR Sant Feliu	72h	
No	Estado EBARs existentes	EBAR	EBAR Can Rafamans	Bombeo	Estado bombas, averias, caudal bombeado, etc...	30	EBAR Can Rafamans	5 min	5 min	Decimal	PLC Pooling EDAR Sant Feliu	EDAR Sant Feliu	72h	
No	Estado EBARs existentes	EBAR	EBAR Torrelles (Can Güell)	Bombeo	Estado bombas, averias, caudal bombeado, etc...	30	EBAR Torrelles (Can Güell)	5 min	5 min	Decimal	PLC Pooling EDAR Sant Feliu	EDAR Sant Feliu	72h	
No	Estado EBARs existentes	EBAR	EBAR Can Guitart	Bombeo	Estado bombas, averias, caudal bombeado, etc...	30	EBAR Can Guitart	5 min	5 min	Decimal	PLC Pooling EDAR Sant Feliu	EDAR Sant Feliu	72h	
No	Estado EBARs existentes	EBAR	EBAR Can Avellaner	Bombeo	Estado bombas, averias, caudal bombeado, etc...	30	EBAR Can Avellaner	5 min	5 min	Decimal	PLC Pooling EDAR Sant Feliu	EDAR Sant Feliu	72h	
No	Estado EBARs existentes	EBAR	EBAR Sant Cugat 2	Bombeo	Estado bombas, averias, caudal bombeado, etc...	30	EBAR Sant Cugat 2	5 min	5 min	Decimal	PLC Pooling EDAR Vallvidrera	EDAR Sant Feliu	72h	
No	Estado EBARs existentes	EBAR	EBAR Sant Cugat 3	Bombeo	Estado bombas, averias, caudal bombeado, etc...	30	EBAR Sant Cugat 3	5 min	5 min	Decimal	PLC Pooling EDAR Vallvidrera	EDAR Sant Feliu	72h	
No	Estado EBARs existentes	EBAR	EBAR Sant Cugat 4	Bombeo	Estado bombas, averias, caudal bombeado, etc...	30	EBAR Sant Cugat 4	5 min	5 min	Decimal	PLC Pooling EDAR Vallvidrera	EDAR Sant Feliu	72h	
No	Estado EBARs existentes	EBAR	EBAR Sant Cugat 1	Bombeo	Estado bombas, averias, caudal bombeado, etc...	30	EBAR Sant Cugat 1	5 min	5 min	Decimal	PLC Pooling EDAR Vallvidrera	EDAR Sant Feliu	72h	
No	Estado EBARs existentes	EBAR	EBAR Sant Cugat 5	Bombeo	Estado bombas, averias, caudal bombeado, etc...	30	EBAR Sant Cugat 5	5 min	5 min	Decimal	PLC Pooling EDAR Vallvidrera	EDAR Sant Feliu	72h	
No	Estado EBARs existentes	EBAR	EBAR Bellavista	Bombeo	Estado bombas, averias, caudal bombeado, etc...	30	EBAR Bellavista	5 min	5 min	Decimal	PLC Pooling EDAR Vallvidrera	EDAR Sant Feliu	72h	1131
Sí	Calidad de vertido	EQ Castellbisbal	EQ Castellbisbal	Controlador SC4500	Conduct, temp, ph, turbidez	4	EQ Castellbisbal	5 min	5 min	Decimal	PLC Pooling EDAR Sant Feliu	EDAR Sant Feliu	72h	
Sí	Aguas de mar	RED COLECTORES	Colectores pozos de registro (3ud)	Colectores pozos de registro (3ud)	Conductividad	3	Colectores pozos de registro (3ud)	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Aguas de mar	RED COLECTORES	PT-04-00-PR-29 Calle 6	PT-04-00-PR-29 Calle 6	Conductividad	1	PT-04-00-PR-29 Calle 6	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Aguas de mar	RED COLECTORES	PT-04-00-PR-44 Calle 6	PT-04-00-PR-44 Calle 6	Conductividad	1	PT-04-00-PR-44 Calle 6	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Aguas de mar	RED COLECTORES	PT-04-00-SB-59 Calle 3	PT-04-00-SB-59 Calle 3	Conductividad	1	PT-04-00-SB-59 Calle 3	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	MULTISONDA1	EBAR	EBAR CAN GUITART	MULTISONDA1	MULTISONDA1	4	EBAR CAN GUITART	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Sant Feliu	EDAR Sant Feliu	72h	
Sí	MULTISONDA1	EBAR	EBAR CAN PALET	MULTISONDA1	MULTISONDA1	4	EBAR CAN PALET	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Sant Feliu	EDAR Sant Feliu	72h	
Sí	MULTISONDA2	EBAR	EBAR RAFAMANS	MULTISONDA2	MULTISONDA2	4	EBAR RAFAMANS	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Sant Feliu	EDAR Sant Feliu	72h	
Sí	MULTISONDA1	EBAR	EBAR SANT BARTOMEU	MULTISONDA1	MULTISONDA1	4	EBAR SANT BARTOMEU	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Sant Feliu	EDAR Sant Feliu	72h	
Sí	MULTISONDA1	EBAR	EBAR VALLPINEDA 2	MULTISONDA1	MULTISONDA1	4	EBAR VALLPINEDA 2	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Sant Feliu	EDAR Vallvidrera	72h	
Sí	DATA_COND	EBAR	SF-02-03-CB_SB-66 Can Cases	DATA_COND	Conductividad	1	SF-02-03-CB_SB-66 Can Cases	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Sant Feliu	72h	
Sí	DATA_COND	EBAR	SF-03-06-PR-77 Riera cervelló	DATA_COND	Conductividad	1	SF-03-06-PR-77 Riera cervelló	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Sant Feliu	72h	
Sí	DATA_COND	EBAR	SF-03-08-PR-50 Riera Torrelles	DATA_COND	Conductividad	1	SF-03-08-PR-50 Riera Torrelles	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Sant Feliu	72h	
Sí	PLUVIOMETRO	EBAR	EBAR Ca n'Armengol	PLUVIOMETRO	PLUVIOMETRO	4	EBAR Ca n'Armengol	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Sant Feliu	EDAR Sant Feliu	72h	
Sí	PLUVIOMETRO	EBAR	EBAR Can Güell	PLUVIOMETRO	PLUVIOMETRO	4	EBAR Can Güell	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Sant Feliu	EDAR Sant Feliu	72h	
Sí	PLUVIOMETRO	EDAR	EDAR St Feliu	PLUVIOMETRO	PLUVIOMETRO	4	EDAR St Feliu	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Sant Feliu	EDAR Sant Feliu	72h	
Sí	PLUVIOMETRO	EDAR	EBAR Prat	PLUVIOMETRO	PLUVIOMETRO	4	EBAR Prat	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
No	PLUVIOMETROS Colectores		Varias	PLUVIOMETROS Colectores	PLUVIOMETROS Colectores	60	Varias	5 min	8 horas / 5 min	Decimal		EDAR Prat	72h	
Sí	CAUDAL_LASER	EDAR	EDAR EL PRAT (Entrada lado Barcelona)		Caudal entrada EDAR	1	PLC Pooling EDAR Prat	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	CAUDAL_LASER	EDAR	EDAR EL PRAT (Entrada lado Prat)		Caudal entrada EDAR	1	PLC Pooling EDAR Prat	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	CAUDAL_LASER	EDAR	EDAR GAVÀ (Entrada)		Caudal entrada EDAR	1	PLC Pretratamiento EDAR Gavà	5 min	8 horas / 5 min	Decimal	PLC Pretratamiento EDAR Gavà	EDAR Gavá	72h	

Nuevo	Tipo de equipo	Tipo de sede	Nombre sede	Nombre equipo /		Variable /	Numero	Nombre PLC/Datalogger	Frecuencia	Frecuencia envio	Volumen neto dato	Origen del dato/calculo	Ubicación	Capacidad	Total
Sí	CAUDAL_LASER_SUM	EDAR	EDAR SANT FELIU (Entrada)			Caudal entrada EDAR	1	PLC Pretratamiento EDAR Sant Feliu	5 min	8 horas / 5 min	Decimal	PLC Pretratamiento EDAR Sant Feliu	EDAR Sant Feliu	72h	
Sí	HACH_AN_AMONIO_1K	EDAR	EDAR EL PRAT (Entrada lado Barcelona)	HACH_AN_AMONIO_1K		EQS entrada EDAR	1	PLC Pooling EDAR Prat	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	HACH_SON_COND	EDAR	EDAR EL PRAT (Entrada lado Barcelona)	HACH_SON_COND		EQS entrada EDAR	1	PLC Pooling EDAR Prat	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	HACH_SON_ODIS	EDAR	EDAR EL PRAT (Entrada lado Barcelona)	HACH_SON_ODIS		EQS entrada EDAR	1	PLC Pooling EDAR Prat	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	HACH_SON_PH	EDAR	EDAR EL PRAT (Entrada lado Barcelona)	HACH_SON_PH		EQS entrada EDAR	1	PLC Pooling EDAR Prat	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	HACH_SON_REDOX	EDAR	EDAR EL PRAT (Entrada lado Barcelona)	HACH_SON_REDOX		EQS entrada EDAR	1	PLC Pooling EDAR Prat	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	HACH_SON_TUSS	EDAR	EDAR EL PRAT (Entrada lado Barcelona)	HACH_SON_TUSS		EQS entrada EDAR	1	PLC Pooling EDAR Prat	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	HACH_AN_AMONIO_1K	EDAR	EDAR EL PRAT (Entrada lado Prat)	HACH_AN_AMONIO_1K		EQS entrada EDAR	1	PLC Pooling EDAR Prat	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	HACH_SON_COND	EDAR	EDAR EL PRAT (Entrada lado Prat)	HACH_SON_COND		EQS entrada EDAR	1	PLC Pooling EDAR Prat	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	HACH_SON_ODIS	EDAR	EDAR EL PRAT (Entrada lado Prat)	HACH_SON_ODIS		EQS entrada EDAR	1	PLC Pooling EDAR Prat	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	HACH_SON_PH	EDAR	EDAR EL PRAT (Entrada lado Prat)	HACH_SON_PH		EQS entrada EDAR	1	PLC Pooling EDAR Prat	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	HACH_SON_REDOX	EDAR	EDAR EL PRAT (Entrada lado Prat)	HACH_SON_REDOX		EQS entrada EDAR	1	PLC Pooling EDAR Prat	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	HACH_SON_TUSS	EDAR	EDAR EL PRAT (Entrada lado Prat)	HACH_SON_TUSS		EQS entrada EDAR	1	PLC Pooling EDAR Prat	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	HACH_AN_AMONIO_1K	EDAR	EDAR GAVÀ (Entrada)	HACH_AN_AMONIO_1K		EQS entrada EDAR	1	PLC Pretratamiento EDAR Gavà	5 min	8 horas / 5 min	Decimal	PLC Pretratamiento EDAR Gavà	EDAR Gavá	72h	
Sí	HACH_SON_ODIS	EDAR	EDAR GAVÀ (Entrada)	HACH_SON_ODIS		EQS entrada EDAR	1	PLC Pretratamiento EDAR Gavà	5 min	8 horas / 5 min	Decimal	PLC Pretratamiento EDAR Gavà	EDAR Gavá	72h	
Sí	HACH_SON_REDOX	EDAR	EDAR GAVÀ (Entrada)	HACH_SON_REDOX		EQS entrada EDAR	1	PLC Pretratamiento EDAR Gavà	5 min	8 horas / 5 min	Decimal	PLC Pretratamiento EDAR Gavà	EDAR Gavá	72h	
Sí	HACH_SON_TUSS	EDAR	EDAR GAVÀ (Entrada)	HACH_SON_TUSS		EQS entrada EDAR	1	PLC Pretratamiento EDAR Gavà	5 min	8 horas / 5 min	Decimal	PLC Pretratamiento EDAR Gavà	EDAR Gavá	72h	
Sí	HACH_AN_AMONIO_1K	EDAR	EDAR SANT FELIU (Entrada)	HACH_AN_AMONIO_1K		EQS entrada EDAR	1	PLC Pretratamiento EDAR Sant Feliu	5 min	8 horas / 5 min	Decimal	PLC Pretratamiento EDAR Sant Feliu	EDAR Sant Feliu	72h	
Sí	HACH_SON_COND	EDAR	EDAR SANT FELIU (Entrada)	HACH_SON_COND		EQS entrada EDAR	1	PLC Pretratamiento EDAR Sant Feliu	5 min	8 horas / 5 min	Decimal	PLC Pretratamiento EDAR Sant Feliu	EDAR Sant Feliu	72h	
Sí	HACH_SON_ODIS	EDAR	EDAR SANT FELIU (Entrada)	HACH_SON_ODIS		EQS entrada EDAR	1	PLC Pretratamiento EDAR Sant Feliu	5 min	8 horas / 5 min	Decimal	PLC Pretratamiento EDAR Sant Feliu	EDAR Sant Feliu	72h	
Sí	HACH_SON_REDOX	EDAR	EDAR SANT FELIU (Entrada)	HACH_SON_REDOX		EQS entrada EDAR	1	PLC Pretratamiento EDAR Sant Feliu	5 min	8 horas / 5 min	Decimal	PLC Pretratamiento EDAR Sant Feliu	EDAR Sant Feliu	72h	
Sí	HACH_SON_TUSS	EDAR	EDAR SANT FELIU (Entrada)	HACH_SON_TUSS		EQS entrada EDAR	1	PLC Pretratamiento EDAR Sant Feliu	5 min	8 horas / 5 min	Decimal	PLC Pretratamiento EDAR Sant Feliu	EDAR Sant Feliu	72h	
No	Sonda pH	EDAR	EDAR Gavá	Sonda pH		pH	1	PLC Pretratamiento EDAR Gavà	5 min	8 horas / 5 min	Decimal	PLC Pretratamiento EDAR Gavà	EDAR Gavá	72h	
No	Sonda Conductividad y temp	EDAR	EDAR Gavá	Sonda Conductividad y temp		Conductividad	1	PLC Pretratamiento EDAR Gavà	5 min	8 horas / 5 min	Decimal	PLC Pretratamiento EDAR Gavà	EDAR Gavá	72h	
No	Sonda Conductividad y temp	EDAR	EDAR Gavá	Sonda Conductividad y temp		Temperatura	1	PLC Pretratamiento EDAR Gavà	5 min	8 horas / 5 min	Decimal	PLC Pretratamiento EDAR Gavà	EDAR Gavá	72h	
No	Sonda pH	EDAR	EDAR Sant Feliu	Sonda pH		pH	1	PLC Pretratamiento EDAR Sant Feliu	5 min	8 horas / 5 min	Decimal	PLC Pretratamiento EDAR Sant Feliu	EDAR Sant Feliu	72h	4
Sí	Analizador de energía	EDAR	EDAR Prat		81	40	3240	PLC Pooling EDAR Prat	15 minutos	5 minuto	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	Analizador de energía	EBAR	EBAR Avantport Sud		6	40	240	PLC Pooling EDAR Prat	15 minutos	5 minuto	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	Analizador de energía	EDAR	EDAR Gavá		30	40	1200	PLC Pretratamiento EDAR Gavà	15 minutos	5 minuto	Decimal	PLC Pretratamiento EDAR Gavà	EDAR Gavá	72h	
Sí	Analizador de energía	EDAR	EDAR Sant Feliu		16	40	640	PLC Pretratamiento EDAR Sant Feliu	15 minutos	5 minuto	Decimal	PLC Pretratamiento EDAR Sant Feliu	EDAR Sant Feliu	72h	
No	Analizador de energía	EDAR	EDAR Prat		30	40	1200	PLC Pooling EDAR Prat	15 minutos	5 minuto	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
No	Analizador de energía	EDAR	EDAR Gavá		40	40	1600	PLC Pretratamiento EDAR Gavà	15 minutos	5 minuto	Decimal	PLC Pretratamiento EDAR Gavà	EDAR Gavá	72h	
No	Analizador de energía	EDAR	EDAR Sant Feliu		36	40	1440	PLC Pretratamiento EDAR Sant Feliu	15 minutos	5 minuto	Decimal	PLC Pretratamiento EDAR Sant Feliu	EDAR Sant Feliu	72h	9560
Sí	Caudalimetro	RED COLECTORES	BS-03-00-PR_CN_SB-20	BS-03-00-PR_CN_SB-20		Nivel	1	BS-03-00-PR_CN_SB-20	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	BS-03-00-PR_CN_SB-20	BS-03-00-PR_CN_SB-20		Velocidad superficial	1	BS-03-00-PR_CN_SB-20	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	BS-03-00-PR_CN_SB-20	BS-03-00-PR_CN_SB-20		Caudal	1	BS-03-00-PR_CN_SB-20	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	BS-03-00-PR_SB-41	BS-03-00-PR_SB-41		Nivel	1	BS-03-00-PR_SB-41	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	BS-03-00-PR_SB-41	BS-03-00-PR_SB-41		Velocidad superficial	1	BS-03-00-PR_SB-41	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	BS-03-00-PR_SB-41	BS-03-00-PR_SB-41		Caudal	1	BS-03-00-PR_SB-41	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	BS-02-11-CN_SB-01_3A	BS-02-11-CN_SB-01_3A		Nivel	1	BS-02-11-CN_SB-01_3A	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	BS-02-11-CN_SB-01_3A	BS-02-11-CN_SB-01_3A		Velocidad superficial	1	BS-02-11-CN_SB-01_3A	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	BS-02-11-CN_SB-01_3A	BS-02-11-CN_SB-01_3A		Caudal	1	BS-02-11-CN_SB-01_3A	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	BS-02-08-PR_SB-05	BS-02-08-PR_SB-05		Nivel	1	BS-02-08-PR_SB-05	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	BS-02-08-PR_SB-05	BS-02-08-PR_SB-05		Velocidad superficial	1	BS-02-08-PR_SB-05	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	BS-02-08-PR_SB-05	BS-02-08-PR_SB-05		Caudal	1	BS-02-08-PR_SB-05	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	BS-02-07-PR_SB-01	BS-02-07-PR_SB-01		Nivel	1	BS-02-07-PR_SB-01	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	BS-02-07-PR_SB-01	BS-02-07-PR_SB-01		Velocidad superficial	1	BS-02-07-PR_SB-01	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	BS-02-07-PR_SB-01	BS-02-07-PR_SB-01		Caudal	1	BS-02-07-PR_SB-01	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	BS-02-12-CB_SB-03	BS-02-12-CB_SB-03		Nivel	1	BS-02-12-CB_SB-03	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	BS-02-12-CB_SB-03	BS-02-12-CB_SB-03		Velocidad superficial	1	BS-02-12-CB_SB-03	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	BS-02-12-CB_SB-03	BS-02-12-CB_SB-03		Caudal	1	BS-02-12-CB_SB-03	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	BS-02-00-PR_SB-05	BS-02-00-PR_SB-05		Nivel	1	BS-02-00-PR_SB-05	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	BS-02-00-PR_SB-05	BS-02-00-PR_SB-05		Velocidad superficial	1	BS-02-00-PR_SB-05	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	BS-02-00-PR_SB-05	BS-02-00-PR_SB-05		Caudal	1	BS-02-00-PR_SB-05	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	BS-02-00-PR_SB-168	BS-02-00-PR_SB-168		Nivel	1	BS-02-00-PR_SB-168	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	BS-02-00-PR_SB-168	BS-02-00-PR_SB-168		Velocidad superficial	1	BS-02-00-PR_SB-168	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	BS-02-00-PR_SB-168	BS-02-00-PR_SB-168		Caudal	1	BS-02-00-PR_SB-168	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	GV-02-00-PR_SB-20	GV-02-00-PR_SB-20		Nivel	1	GV-02-00-PR_SB-20	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	GV-02-00-PR_SB-20	GV-02-00-PR_SB-20		Velocidad superficial	1	GV-02-00-PR_SB-20	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	GV-02-00-PR_SB-20	GV-02-00-PR_SB-20		Caudal	1	GV-02-00-PR_SB-20	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	GV-03-02-PR_SB-3.09	GV-03-02-PR_SB-3.09		Nivel	1	GV-03-02-PR_SB-3.09	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	GV-03-02-PR_SB-3.09	GV-03-02-PR_SB-3.09		Velocidad superficial	1	GV-03-02-PR_SB-3.09	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	GV-03-02-PR_SB-3.09	GV-03-02-PR_SB-3.09		Caudal	1	GV-03-02-PR_SB-3.09	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	GV-03-06-PR_SB-10	GV-03-06-PR_SB-10		Nivel	1	GV-03-06-PR_SB-10	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	GV-03-06-PR_SB-10	GV-03-06-PR_SB-10		Velocidad superficial	1	GV-03-06-PR_SB-10	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	GV-03-06-PR_SB-10	GV-03-06-PR_SB-10		Caudal	1	GV-03-06-PR_SB-10	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	GV-03-04-CB_SB-37a	GV-03-04-CB_SB-37a		Nivel	1	GV-03-04-CB_SB-37a	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	GV-03-04-CB_SB-37a	GV-03-04-CB_SB-37a		Velocidad superficial	1	GV-03-04-CB_SB-37a	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	GV-03-04-CB_SB-37a	GV-03-04-CB_SB-37a		Caudal	1	GV-03-04-CB_SB-37a	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	MN-02-03-CN_SB-03	MN-02-03-CN_SB-03		Nivel	1	MN-02-03-CN_SB-03	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	MN-02-03-CN_SB-03	MN-02-03-CN_SB-03		Velocidad superficial	1	MN-02-03-CN_SB-03	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	MN-02-03-CN_SB-03	MN-02-03-CN_SB-03		Caudal	1	MN-02-03-CN_SB-03	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	MN-02-01-PR-01.1	MN-02-01-PR-01.1		Nivel	1	MN-02-01-PR-01.1	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	MN-02-01-PR-01.1	MN-02-01-PR-01.1		Velocidad superficial	1	MN-02-01-PR-01.1	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	MN-02-01-PR-01.1	MN-02-01-PR-01.1		Caudal	1	MN-02-01-PR-01.1	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	MN-04-01-PR_SB-02	MN-04-01-PR_SB-02		Nivel	1	MN-04-01-PR_SB-02	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	MN-04-01-PR_SB-02	MN-04-01-PR_SB-02		Velocidad superficial	1	MN-04-01-PR_SB-02	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	MN-04-01-PR_SB-02	MN-04-01-PR_SB-02		Caudal	1	MN-04-01-PR_SB-02	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	MN-04-03-CN_SB-01	MN-04-03-CN_SB-01		Nivel	1	MN-04-03-CN_SB-01	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	MN-04-03-CN_SB-01	MN-04-03-CN_SB-01		Velocidad superficial	1	MN-04-03-CN_SB-01	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	MN-04-03-CN_SB-01	MN-04-03-CN_SB-01		Caudal	1	MN-04-03-CN_SB-01	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-04-01-PR_SBb-07	PT-04-01-PR_SBb-07		Nivel	1	PT-04-01-PR_SBb-07	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-04-01-PR_SBb-07	PT-04-01-PR_SBb-07		Velocidad superficial	1	PT-04-01-PR_SBb-07	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-04-01-PR_SBb-07	PT-04-01-PR_SBb-07		Caudal	1	PT-04-01-PR_SBb-07	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-04-00-PR_SB-115	PT-04-00-PR_SB-115		Nivel	1	PT-04-00-PR_SB-115	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-04-00-PR_SB-115	PT-04-00-PR_SB-115		Velocidad superficial	1	PT-04-00-PR_SB-115	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-04-00-PR_SB-115	PT-04-00-PR_SB-115		Caudal	1	PT-04-00-PR_SB-115	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-02-05-PR_SB-09a	PT-02-05-PR_SB-09a		Nivel	1	PT-02-05-PR_SB-09a	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-02-05-PR_SB-09a	PT-02-05-PR_SB-09a		Velocidad superficial	1	PT-02-05-PR_SB-09a	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-02-05-PR_SB-09a	PT-02-05-PR_SB-09a		Caudal	1	PT-02-05-PR_SB-09a	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-02-04-PR_SB-13	PT-02-04-PR_SB-13		Nivel	1	PT-02-04-PR_SB-13	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	

Nuevo	Tipo de equipo	Tipo de sede	Nombre sede	Nombre equipo /	Variable /	Numero	Nombre PLC/Datalogger	Frecuencia	Frecuencia envio	Volumen neto dato	Origen del dato/calculo	Ubicación	Capacidad	Total
Sí	Caudalimetro	RED COLECTORES	PT-02-04-PR_SB-13	PT-02-04-PR_SB-13	Velocidad superficial	1	PT-02-04-PR_SB-13	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-02-04-PR_SB-13	PT-02-04-PR_SB-13	Caudal	1	PT-02-04-PR_SB-13	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-02-02-PR_SB-01	PT-02-02-PR_SB-01	Nivel	1	PT-02-02-PR_SB-01	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-02-02-PR_SB-01	PT-02-02-PR_SB-01	Velocidad superficial	1	PT-02-02-PR_SB-01	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-02-02-PR_SB-01	PT-02-02-PR_SB-01	Caudal	1	PT-02-02-PR_SB-01	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-01-00-CB_SB-70	PT-01-00-CB_SB-70	Nivel	1	PT-01-00-CB_SB-70	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-01-00-CB_SB-70	PT-01-00-CB_SB-70	Velocidad superficial	1	PT-01-00-CB_SB-70	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-01-00-CB_SB-70	PT-01-00-CB_SB-70	Caudal	1	PT-01-00-CB_SB-70	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-03-05-PR_SB-06	PT-03-05-PR_SB-06	Nivel	1	PT-03-05-PR_SB-06	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-03-05-PR_SB-06	PT-03-05-PR_SB-06	Velocidad superficial	1	PT-03-05-PR_SB-06	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-03-05-PR_SB-06	PT-03-05-PR_SB-06	Caudal	1	PT-03-05-PR_SB-06	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-03-03-PRp_SB-13	PT-03-03-PRp_SB-13	Nivel	1	PT-03-03-PRp_SB-13	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-03-03-PRp_SB-13	PT-03-03-PRp_SB-13	Velocidad superficial	1	PT-03-03-PRp_SB-13	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-03-03-PRp_SB-13	PT-03-03-PRp_SB-13	Caudal	1	PT-03-03-PRp_SB-13	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-03-03-PR_SB-17	PT-03-03-PR_SB-17	Nivel	1	PT-03-03-PR_SB-17	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-03-03-PR_SB-17	PT-03-03-PR_SB-17	Velocidad superficial	1	PT-03-03-PR_SB-17	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-03-03-PR_SB-17	PT-03-03-PR_SB-17	Caudal	1	PT-03-03-PR_SB-17	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-03-01-CB_CN_SB-02	PT-03-01-CB_CN_SB-02	Nivel	1	PT-03-01-CB_CN_SB-02	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-03-01-CB_CN_SB-02	PT-03-01-CB_CN_SB-02	Velocidad superficial	1	PT-03-01-CB_CN_SB-02	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-03-01-CB_CN_SB-02	PT-03-01-CB_CN_SB-02	Caudal	1	PT-03-01-CB_CN_SB-02	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-03-01-PR_SB-41	PT-03-01-PR_SB-41	Nivel	1	PT-03-01-PR_SB-41	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-03-01-PR_SB-41	PT-03-01-PR_SB-41	Velocidad superficial	1	PT-03-01-PR_SB-41	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-03-01-PR_SB-41	PT-03-01-PR_SB-41	Caudal	1	PT-03-01-PR_SB-41	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-01-08-PR_SB-02	PT-01-08-PR_SB-02	Nivel	1	PT-01-08-PR_SB-02	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-01-08-PR_SB-02	PT-01-08-PR_SB-02	Velocidad superficial	1	PT-01-08-PR_SB-02	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-01-08-PR_SB-02	PT-01-08-PR_SB-02	Caudal	1	PT-01-08-PR_SB-02	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-01-08-PR_SB-22	PT-01-08-PR_SB-22	Nivel	1	PT-01-08-PR_SB-22	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-01-08-PR_SB-22	PT-01-08-PR_SB-22	Velocidad superficial	1	PT-01-08-PR_SB-22	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-01-08-PR_SB-22	PT-01-08-PR_SB-22	Caudal	1	PT-01-08-PR_SB-22	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-01-08-PR_SB-28	PT-01-08-PR_SB-28	Nivel	1	PT-01-08-PR_SB-28	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-01-08-PR_SB-28	PT-01-08-PR_SB-28	Velocidad superficial	1	PT-01-08-PR_SB-28	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-01-08-PR_SB-28	PT-01-08-PR_SB-28	Caudal	1	PT-01-08-PR_SB-28	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-01-09-PR_SB-04	PT-01-09-PR_SB-04	Nivel	1	PT-01-09-PR_SB-04	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-01-09-PR_SB-04	PT-01-09-PR_SB-04	Velocidad superficial	1	PT-01-09-PR_SB-04	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-01-09-PR_SB-04	PT-01-09-PR_SB-04	Caudal	1	PT-01-09-PR_SB-04	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-02-08-SB	PT-02-08-SB	Nivel	1	PT-02-08-SB	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-02-08-SB	PT-02-08-SB	Velocidad superficial	1	PT-02-08-SB	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	PT-02-08-SB	PT-02-08-SB	Caudal	1	PT-02-08-SB	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-05-00-PR_SB-01	SF-05-00-PR_SB-01	Nivel	1	SF-05-00-PR_SB-01	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-05-00-PR_SB-01	SF-05-00-PR_SB-01	Velocidad superficial	1	SF-05-00-PR_SB-01	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-05-00-PR_SB-01	SF-05-00-PR_SB-01	Caudal	1	SF-05-00-PR_SB-01	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-05-00-CB_SB-07	SF-05-00-CB_SB-07	Nivel	1	SF-05-00-CB_SB-07	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-05-00-CB_SB-07	SF-05-00-CB_SB-07	Velocidad superficial	1	SF-05-00-CB_SB-07	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-05-00-CB_SB-07	SF-05-00-CB_SB-07	Caudal	1	SF-05-00-CB_SB-07	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-01-00-SI_SB-01	SF-01-00-SI_SB-01	Nivel	1	SF-01-00-SI_SB-01	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-01-00-SI_SB-01	SF-01-00-SI_SB-01	Velocidad superficial	1	SF-01-00-SI_SB-01	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-01-00-SI_SB-01	SF-01-00-SI_SB-01	Caudal	1	SF-01-00-SI_SB-01	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-05-00-PR_SB-39	SF-05-00-PR_SB-39	Nivel	1	SF-05-00-PR_SB-39	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-05-00-PR_SB-39	SF-05-00-PR_SB-39	Velocidad superficial	1	SF-05-00-PR_SB-39	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-05-00-PR_SB-39	SF-05-00-PR_SB-39	Caudal	1	SF-05-00-PR_SB-39	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-01-00-CB_SB-63	SF-01-00-CB_SB-63	Nivel	1	SF-01-00-CB_SB-63	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-01-00-CB_SB-63	SF-01-00-CB_SB-63	Velocidad superficial	1	SF-01-00-CB_SB-63	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-01-00-CB_SB-63	SF-01-00-CB_SB-63	Caudal	1	SF-01-00-CB_SB-63	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-02-00-CB_SB-58	SF-02-00-CB_SB-58	Nivel	1	SF-02-00-CB_SB-58	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-02-00-CB_SB-58	SF-02-00-CB_SB-58	Velocidad superficial	1	SF-02-00-CB_SB-58	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-02-00-CB_SB-58	SF-02-00-CB_SB-58	Caudal	1	SF-02-00-CB_SB-58	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-04-00-PR_SB-54	SF-04-00-PR_SB-54	Nivel	1	SF-04-00-PR_SB-54	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-04-00-PR_SB-54	SF-04-00-PR_SB-54	Velocidad superficial	1	SF-04-00-PR_SB-54	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-04-00-PR_SB-54	SF-04-00-PR_SB-54	Caudal	1	SF-04-00-PR_SB-54	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-04-02-PR_SB-04	SF-04-02-PR_SB-04	Nivel	1	SF-04-02-PR_SB-04	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-04-02-PR_SB-04	SF-04-02-PR_SB-04	Velocidad superficial	1	SF-04-02-PR_SB-04	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-04-02-PR_SB-04	SF-04-02-PR_SB-04	Caudal	1	SF-04-02-PR_SB-04	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-04-05-PR_SB-12	SF-04-05-PR_SB-12	Nivel	1	SF-04-05-PR_SB-12	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-04-05-PR_SB-12	SF-04-05-PR_SB-12	Velocidad superficial	1	SF-04-05-PR_SB-12	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-04-05-PR_SB-12	SF-04-05-PR_SB-12	Caudal	1	SF-04-05-PR_SB-12	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-04-08-PR_SB-06	SF-04-08-PR_SB-06	Nivel	1	SF-04-08-PR_SB-06	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-04-08-PR_SB-06	SF-04-08-PR_SB-06	Velocidad superficial	1	SF-04-08-PR_SB-06	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-04-08-PR_SB-06	SF-04-08-PR_SB-06	Caudal	1	SF-04-08-PR_SB-06	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-03-16-PR-CN-SB-04	SF-03-16-PR-CN-SB-04	Nivel	1	SF-03-16-PR-CN-SB-04	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-03-16-PR-CN-SB-04	SF-03-16-PR-CN-SB-04	Velocidad superficial	1	SF-03-16-PR-CN-SB-04	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-03-16-PR-CN-SB-04	SF-03-16-PR-CN-SB-04	Caudal	1	SF-03-16-PR-CN-SB-04	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-04-00-PR_SB-06	SF-04-00-PR_SB-06	Nivel	1	SF-04-00-PR_SB-06	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-04-00-PR_SB-06	SF-04-00-PR_SB-06	Velocidad superficial	1	SF-04-00-PR_SB-06	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-04-00-PR_SB-06	SF-04-00-PR_SB-06	Caudal	1	SF-04-00-PR_SB-06	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-03-00-SI_SB-10	SF-03-00-SI_SB-10	Nivel	1	SF-03-00-SI_SB-10	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-03-00-SI_SB-10	SF-03-00-SI_SB-10	Velocidad superficial	1	SF-03-00-SI_SB-10	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-03-00-SI_SB-10	SF-03-00-SI_SB-10	Caudal	1	SF-03-00-SI_SB-10	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-03-08-PR_SB-04	SF-03-08-PR_SB-04	Nivel	1	SF-03-08-PR_SB-04	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-03-08-PR_SB-04	SF-03-08-PR_SB-04	Velocidad superficial	1	SF-03-08-PR_SB-04	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-03-08-PR_SB-04	SF-03-08-PR_SB-04	Caudal	1	SF-03-08-PR_SB-04	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-03-07-PR_CN_SB-01	SF-03-07-PR_CN_SB-01	Nivel	1	SF-03-07-PR_CN_SB-01	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-03-07-PR_CN_SB-01	SF-03-07-PR_CN_SB-01	Velocidad superficial	1	SF-03-07-PR_CN_SB-01	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-03-07-PR_CN_SB-01	SF-03-07-PR_CN_SB-01	Caudal	1	SF-03-07-PR_CN_SB-01	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-03-13-PR_SB-06	SF-03-13-PR_SB-06	Nivel	1	SF-03-13-PR_SB-06	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-03-13-PR_SB-06	SF-03-13-PR_SB-06	Velocidad superficial	1	SF-03-13-PR_SB-06	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-03-13-PR_SB-06	SF-03-13-PR_SB-06	Caudal	1	SF-03-13-PR_SB-06	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-03-16-PR_SB-29	SF-03-16-PR_SB-29	Nivel	1	SF-03-16-PR_SB-29	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-03-16-PR_SB-29	SF-03-16-PR_SB-29	Velocidad superficial	1	SF-03-16-PR_SB-29	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-03-16-PR_SB-29	SF-03-16-PR_SB-29	Caudal	1	SF-03-16-PR_SB-29	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-02-07-CN_SB-05.1	SF-02-07-CN_SB-05.1	Nivel	1	SF-02-07-CN_SB-05.1	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
Sí	Caudalimetro	RED COLECTORES	SF-02-07-CN_SB-05.1	SF-02-07-CN_SB-05.1	Velocidad superficial	1	SF-02-07-CN_SB-05.1	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	

Nuevo	Tipo de equipo	Tipo de sede	Nombre sede	Nombre equipo /	Variable /	Numero	Nombre PLC/Datalogger	Frecuencia	Frecuencia envio	Volumen neto dato	Origen del dato/calculo	Ubicación	Capacidad	Total
Sí	Caudalimetro	RED COLECTORES	SF-02-07-CN_SB-05.1	SF-02-07-CN_SB-05.1	Caudal	1	SF-02-07-CN_SB-05.1	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	BS-02-00-SB-14	BS-02-00-SB-14	Nivel	1	BS-02-00-SB-14	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	BS-02-00-SB-14	BS-02-00-SB-14	Velocidad superficial	1	BS-02-00-SB-14	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	BS-02-00-SB-14	BS-02-00-SB-14	Caudal	1	BS-02-00-SB-14	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	BS-03-00-PR_SB-02.1	BS-03-00-PR_SB-02.1	Nivel	1	BS-03-00-PR_SB-02.1	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	BS-03-00-PR_SB-02.1	BS-03-00-PR_SB-02.1	Velocidad superficial	1	BS-03-00-PR_SB-02.1	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	BS-03-00-PR_SB-02.1	BS-03-00-PR_SB-02.1	Caudal	1	BS-03-00-PR_SB-02.1	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	BS-02-11-CN_SB-01_3B	BS-02-11-CN_SB-01_3B	Nivel	1	BS-02-11-CN_SB-01_3B	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	BS-02-11-CN_SB-01_3B	BS-02-11-CN_SB-01_3B	Velocidad superficial	1	BS-02-11-CN_SB-01_3B	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	BS-02-11-CN_SB-01_3B	BS-02-11-CN_SB-01_3B	Caudal	1	BS-02-11-CN_SB-01_3B	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	BS-02-10-PR_SB-03	BS-02-10-PR_SB-03	Nivel	1	BS-02-10-PR_SB-03	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	BS-02-10-PR_SB-03	BS-02-10-PR_SB-03	Velocidad superficial	1	BS-02-10-PR_SB-03	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	BS-02-10-PR_SB-03	BS-02-10-PR_SB-03	Caudal	1	BS-02-10-PR_SB-03	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	BS-02-00-PR_SB-66.3	BS-02-00-PR_SB-66.3	Nivel	1	BS-02-00-PR_SB-66.3	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	BS-02-00-PR_SB-66.3	BS-02-00-PR_SB-66.3	Velocidad superficial	1	BS-02-00-PR_SB-66.3	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	BS-02-00-PR_SB-66.3	BS-02-00-PR_SB-66.3	Caudal	1	BS-02-00-PR_SB-66.3	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	BS-02-06-CN_SB-00	BS-02-06-CN_SB-00	Nivel	1	BS-02-06-CN_SB-00	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	BS-02-06-CN_SB-00	BS-02-06-CN_SB-00	Velocidad superficial	1	BS-02-06-CN_SB-00	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	BS-02-06-CN_SB-00	BS-02-06-CN_SB-00	Caudal	1	BS-02-06-CN_SB-00	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	BS-02-02-DE_SB-03.2	BS-02-02-DE_SB-03.2	Nivel	1	BS-02-02-DE_SB-03.2	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	BS-02-02-DE_SB-03.2	BS-02-02-DE_SB-03.2	Velocidad superficial	1	BS-02-02-DE_SB-03.2	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	BS-02-02-DE_SB-03.2	BS-02-02-DE_SB-03.2	Caudal	1	BS-02-02-DE_SB-03.2	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	22
No	Caudalimetro	RED COLECTORES	GV-04-01-PR_SB-63	GV-04-01-PR_SB-63	Nivel	1	GV-04-01-PR_SB-63	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	GV-04-01-PR_SB-63	GV-04-01-PR_SB-63	Velocidad superficial	1	GV-04-01-PR_SB-63	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	GV-04-01-PR_SB-63	GV-04-01-PR_SB-63	Caudal	1	GV-04-01-PR_SB-63	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	GV-03-03-PR_SB-42	GV-03-03-PR_SB-42	Nivel	1	GV-03-03-PR_SB-42	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	GV-03-03-PR_SB-42	GV-03-03-PR_SB-42	Velocidad superficial	1	GV-03-03-PR_SB-42	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	GV-03-03-PR_SB-42	GV-03-03-PR_SB-42	Caudal	1	GV-03-03-PR_SB-42	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	GV-03-03-PR_SB-52	GV-03-03-PR_SB-52	Nivel	1	GV-03-03-PR_SB-52	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	GV-03-03-PR_SB-52	GV-03-03-PR_SB-52	Velocidad superficial	1	GV-03-03-PR_SB-52	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	GV-03-03-PR_SB-52	GV-03-03-PR_SB-52	Caudal	1	GV-03-03-PR_SB-52	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	GV-03-03-PR_SB-70	GV-03-03-PR_SB-70	Nivel	1	GV-03-03-PR_SB-70	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	GV-03-03-PR_SB-70	GV-03-03-PR_SB-70	Velocidad superficial	1	GV-03-03-PR_SB-70	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	GV-03-03-PR_SB-70	GV-03-03-PR_SB-70	Caudal	1	GV-03-03-PR_SB-70	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	GV-03-03-PR_SB-80	GV-03-03-PR_SB-80	Nivel	1	GV-03-03-PR_SB-80	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	GV-03-03-PR_SB-80	GV-03-03-PR_SB-80	Velocidad superficial	1	GV-03-03-PR_SB-80	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	GV-03-03-PR_SB-80	GV-03-03-PR_SB-80	Caudal	1	GV-03-03-PR_SB-80	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	MN-02-01-CB_CN_SB-01.1	MN-02-01-CB_CN_SB-01.1	Nivel	1	MN-02-01-CB_CN_SB-01.1	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	MN-02-01-CB_CN_SB-01.1	MN-02-01-CB_CN_SB-01.1	Velocidad superficial	1	MN-02-01-CB_CN_SB-01.1	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	MN-02-01-CB_CN_SB-01.1	MN-02-01-CB_CN_SB-01.1	Caudal	1	MN-02-01-CB_CN_SB-01.1	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	PT-04-02-SB-06	PT-04-02-SB-06	Nivel	1	PT-04-02-SB-06	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	PT-04-02-SB-06	PT-04-02-SB-06	Velocidad superficial	1	PT-04-02-SB-06	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	PT-04-02-SB-06	PT-04-02-SB-06	Caudal	1	PT-04-02-SB-06	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	PT-04-00-PR_SB-94	PT-04-00-PR_SB-94	Nivel	1	PT-04-00-PR_SB-94	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	PT-04-00-PR_SB-94	PT-04-00-PR_SB-94	Velocidad superficial	1	PT-04-00-PR_SB-94	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	PT-04-00-PR_SB-94	PT-04-00-PR_SB-94	Caudal	1	PT-04-00-PR_SB-94	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	PT-03-01-PR_SB-20	PT-03-01-PR_SB-20	Nivel	1	PT-03-01-PR_SB-20	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	PT-03-01-PR_SB-20	PT-03-01-PR_SB-20	Velocidad superficial	1	PT-03-01-PR_SB-20	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	PT-03-01-PR_SB-20	PT-03-01-PR_SB-20	Caudal	1	PT-03-01-PR_SB-20	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	SF-05-00-CB_SB-18	SF-05-00-CB_SB-18	Nivel	1	SF-05-00-CB_SB-18	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	SF-05-00-CB_SB-18	SF-05-00-CB_SB-18	Velocidad superficial	1	SF-05-00-CB_SB-18	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	SF-05-00-CB_SB-18	SF-05-00-CB_SB-18	Caudal	1	SF-05-00-CB_SB-18	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	SF-02-00-CB_SB-67	SF-02-00-CB_SB-67	Nivel	1	SF-02-00-CB_SB-67	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	SF-02-00-CB_SB-67	SF-02-00-CB_SB-67	Velocidad superficial	1	SF-02-00-CB_SB-67	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	SF-02-00-CB_SB-67	SF-02-00-CB_SB-67	Caudal	1	SF-02-00-CB_SB-67	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	SF-04-00-CB_SB-44	SF-04-00-CB_SB-44	Nivel	1	SF-04-00-CB_SB-44	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	SF-04-00-CB_SB-44	SF-04-00-CB_SB-44	Velocidad superficial	1	SF-04-00-CB_SB-44	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	SF-04-00-CB_SB-44	SF-04-00-CB_SB-44	Caudal	1	SF-04-00-CB_SB-44	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	SF-02-06-PR_SB-01	SF-02-06-PR_SB-01	Nivel	1	SF-02-06-PR_SB-01	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	SF-02-06-PR_SB-01	SF-02-06-PR_SB-01	Velocidad superficial	1	SF-02-06-PR_SB-01	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	SF-02-06-PR_SB-01	SF-02-06-PR_SB-01	Caudal	1	SF-02-06-PR_SB-01	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	SF-02-03-PR_SB-02	SF-02-03-PR_SB-02	Nivel	1	SF-02-03-PR_SB-02	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	SF-02-03-PR_SB-02	SF-02-03-PR_SB-02	Velocidad superficial	1	SF-02-03-PR_SB-02	5 min	8 horas / 5 min	Decimal	SOFREL PCWin EDAR Prat	EDAR Prat	72h	
No	Caudalimetro	RED COLECTORES	SF-02-03-PR_SB-02	SF-02-03-PR_SB-02	Caudal	1	SF-02-03-PR_SB-02	5 min	8 horas / 5 min	Decimal	Edge El prat	EDAR Prat	72h	
Sí	Caudalimetro	Alivios EBARs	PT-04-02-SB-06	PT-04-02-SB-06	Nivel/Velocidad/Caudal	3	PT-04-02-SB-06	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
Sí	Caudalimetro	Alivios EBARs	PT-04-00-SB-EEBB-Sud (Avantport - Carrer A)	PT-04-00-SB-EEBB-Sud (Avantport - Carrer A)	Nivel/Velocidad/Caudal	3	PT-04-00-SB-EEBB-Sud (Avantport - Carrer A)	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
Sí	Caudalimetro	Alivios EBARs	PT-02-00-PR_SB-04	PT-02-00-PR_SB-04	Nivel/Velocidad/Caudal	3	PT-02-00-PR_SB-04	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
Sí	Caudalimetro	Alivios EBARs	PT-01-01-PR_SB-02	PT-01-01-PR_SB-02	Nivel/Velocidad/Caudal	3	PT-01-01-PR_SB-02	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
Sí	Caudalimetro	Alivios EBARs	SF-01-03-EEBB_ SB_Can_Palet	SF-01-03-EEBB_ SB_Can_Palet	Nivel/Velocidad/Caudal	3	SF-01-03-EEBB_ SB_Can_Palet	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
Sí	Caudalimetro	Alivios EBARs	SF-04-03-EEBB_SB-Sant_Bartomeu	SF-04-03-EEBB_SB-Sant_Bartomeu	Nivel/Velocidad/Caudal	3	SF-04-03-EEBB_SB-Sant_Bartomeu	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
Sí	Caudalimetro	Alivios EBARs	SF-04-06-PR_SB-14	SF-04-06-PR_SB-14	Nivel/Velocidad/Caudal	3	SF-04-06-PR_SB-14	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
Sí	Caudalimetro	Alivios EBARs	SF-04-06-PR_SB-01	SF-04-06-PR_SB-01	Nivel/Velocidad/Caudal	3	SF-04-06-PR_SB-01	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
Sí	Caudalimetro	Alivios EBARs	SF-04-12-PR_SB-01	SF-04-12-PR_SB-01	Nivel/Velocidad/Caudal	3	SF-04-12-PR_SB-01	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
Sí	Caudalimetro	Alivios EBARs	SF-04-12-SB-EEBB-Aigues de Sabadell 5	SF-04-12-SB-EEBB-Aigues de Sabadell 5	Nivel/Velocidad/Caudal	3	SF-04-12-SB-EEBB-Aigues de Sabadell 5	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
Sí	Caudalimetro	Alivios EBARs	SF-03-19-EB-SB-01	SF-03-19-EB-SB-01	Nivel/Velocidad/Caudal	3	SF-03-19-EB-SB-01	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
Sí	Caudalimetro	Alivios EBARs	SF-03-12-PR_SB-02	SF-03-12-PR_SB-02	Nivel/Velocidad/Caudal	3	SF-03-12-PR_SB-02	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
Sí	Caudalimetro	Alivios EBARs	SF-EEBB_SB-Carrer_del_Pi	SF-EEBB_SB-Carrer_del_Pi	Nivel/Velocidad/Caudal	3	SF-EEBB_SB-Carrer_del_Pi	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
Sí	Caudalimetro	Alivios EBARs	SF-EEBB_SB-Placa_de_Avellaner	SF-EEBB_SB-Placa_de_Avellaner	Nivel/Velocidad/Caudal	3	SF-EEBB_SB-Placa_de_Avellaner	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
Sí	Caudalimetro	Alivios EBARs	SF-03-14-EEBB_SB_Rafamans-57	SF-03-14-EEBB_SB_Rafamans-57	Nivel/Velocidad/Caudal	3	SF-03-14-EEBB_SB_Rafamans-57	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
Sí	Caudalimetro	Alivios EBARs	GV-02-00-PR_SB-20	GV-02-00-PR_SB-20	Nivel/Velocidad/Caudal	3	GV-02-00-PR_SB-20	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
Sí	Caudalimetro	Alivios EBARs	GV-02-00-SB-EEBB-Costa Gava-01	GV-02-00-SB-EEBB-Costa Gava-01	Nivel/Velocidad/Caudal	3	GV-02-00-SB-EEBB-Costa Gava-01	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
Sí	Caudalimetro	Alivios EBARs	GV-04-00-SB-EEBB-Costa Castelldefels-01	GV-04-00-SB-EEBB-Costa Castelldefels-01	Nivel/Velocidad/Caudal	3	GV-04-00-SB-EEBB-Costa Castelldefels-01	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
Sí	Caudalimetro	Alivios EBARs	GV-04-01-SB-EEBB-Costa Castelldefels-02	GV-04-01-SB-EEBB-Costa Castelldefels-02	Nivel/Velocidad/Caudal	3	GV-04-01-SB-EEBB-Costa Castelldefels-02	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
Sí	Caudalimetro	Alivios EBARs	GV-04-01-SB-EEBB-Costa Castelldefels-04	GV-04-01-SB-EEBB-Costa Castelldefels-04	Nivel/Velocidad/Caudal	3	GV-04-01-SB-EEBB-Costa Castelldefels-04	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
Sí	Caudalimetro	Alivios EBARs	GV-01-00-SB-EEBB-Interceptor Castelldefels	GV-01-00-SB-EEBB-Interceptor Castelldefels	Nivel/Velocidad/Caudal	3	GV-01-00-SB-EEBB-Interceptor Castelldefels	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
Sí	Caudalimetro	Alivios EBARs	GV-03-07-SB-EEBB-Can Espinós	GV-03-07-SB-EEBB-Can Espinós	Nivel/Velocidad/Caudal	3	GV-03-07-SB-EEBB-Can Espinós	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
Sí	Caudalimetro	Alivios EBARs	GV-03-04-PR_SB-18	GV-03-04-PR_SB-18	Nivel/Velocidad/Caudal	3	GV-03-04-PR_SB-18	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
Sí	Caudalimetro	Alivios EBARs	BS-02-00-SB-14	BS-02-00-SB-14	Nivel/Velocidad/Caudal	3	BS-02-00-SB-14	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
Sí	Caudalimetro	Alivios EBARs	BS-02-04-PR_SB-01	BS-02-04-PR_SB-01	Nivel/Velocidad/Caudal	3	BS-02-04-PR_SB-01	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
Sí	Caudalimetro	Alivios EBARs	BS-02-02-DE_SB-03.2	BS-02-02-DE_SB-03.2	Nivel/Velocidad/Caudal	3	BS-02-02-DE_SB-03.2	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
Sí	Caudalimetro	Alivios EBARs	BS-02-01-EB_SB-06	BS-02-01-EB_SB-06	Nivel/Velocidad/Caudal	3	BS-02-01-EB_SB-06	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	

Nuevo	Tipo de equipo	Tipo de sede	Nombre sede	Nombre equipo /	Variable /	Numero	Nombre PLC/Datalogger	Frecuencia	Frecuencia envio	Volumen neto dato	Origen del dato/calculo	Ubicación	Capacidad	Total
No	Caudalimetros	Alivios EBARs	BS-01-00-PR_SB-21	BS-01-00-PR_SB-21	Nivel/Velocidad/Caudal	3	BS-01-00-PR_SB-21	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
No	Caudalimetros	Alivios EBARs	BS-01-01-SB-EEBB-Ginebra	BS-01-01-SB-EEBB-Ginebra	Nivel/Velocidad/Caudal	3	BS-01-01-SB-EEBB-Ginebra	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
No	Caudalimetros	Alivios EBARs	BS-02-04-PR_SB-01	BS-02-04-PR_SB-01	Nivel/Velocidad/Caudal	3	BS-02-04-PR_SB-01	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
No	Caudalimetros	Alivios EBARs	BS-02-01-EB_SB-06	BS-02-01-EB_SB-06	Nivel/Velocidad/Caudal	3	BS-02-01-EB_SB-06	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
No	Caudalimetros	Alivios EBARs	GV-02-00-SB-EEBB-Costa Gava-01	GV-02-00-SB-EEBB-Costa Gava-01	Nivel/Velocidad/Caudal	3	GV-02-00-SB-EEBB-Costa Gava-01	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
No	Caudalimetros	Alivios EBARs	GV-04-00-SB-EEBB-Costa Castelldefels-01	GV-04-00-SB-EEBB-Costa Castelldefels-01	Nivel/Velocidad/Caudal	3	GV-04-00-SB-EEBB-Costa Castelldefels-01	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
No	Caudalimetros	Alivios EBARs	GV-04-01-SB-EEBB-Costa Castelldefels-02	GV-04-01-SB-EEBB-Costa Castelldefels-02	Nivel/Velocidad/Caudal	3	GV-04-01-SB-EEBB-Costa Castelldefels-02	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
No	Caudalimetros	Alivios EBARs	GV-04-01-SB-EEBB-Costa Castelldefels-04	GV-04-01-SB-EEBB-Costa Castelldefels-04	Nivel/Velocidad/Caudal	3	GV-04-01-SB-EEBB-Costa Castelldefels-04	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
No	Caudalimetros	Alivios EBARs	GV-01-00-SB-EEBB-Interceptor Castelldefels	GV-01-00-SB-EEBB-Interceptor Castelldefels	Nivel/Velocidad/Caudal	3	GV-01-00-SB-EEBB-Interceptor Castelldefels	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
No	Caudalimetros	Alivios EBARs	GV-03-07-SB-EEBB-Can Espinós	GV-03-07-SB-EEBB-Can Espinós	Nivel/Velocidad/Caudal	3	GV-03-07-SB-EEBB-Can Espinós	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
No	Caudalimetros	Alivios EBARs	GV-03-04-PR_SB-18	GV-03-04-PR_SB-18	Nivel/Velocidad/Caudal	3	GV-03-04-PR_SB-18	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
No	Caudalimetros	Alivios EBARs	PT-04-00-SB-EEBB-Sud (Avantport - Carrer A)	PT-04-00-SB-EEBB-Sud (Avantport - Carrer A)	Nivel/Velocidad/Caudal	3	PT-04-00-SB-EEBB-Sud (Avantport - Carrer A)	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
No	Caudalimetros	Alivios EBARs	PT-02-00-PR_SB-04	PT-02-00-PR_SB-04	Nivel/Velocidad/Caudal	3	PT-02-00-PR_SB-04	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
No	Caudalimetros	Alivios EBARs	SF-03-19-EB-SB-01	SF-03-19-EB-SB-01	Nivel/Velocidad/Caudal	3	SF-03-19-EB-SB-01	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
No	Caudalimetros	Alivios EBARs	SF-04-03-EEBB_SB-Sant_Bartomeu	SF-04-03-EEBB_SB-Sant_Bartomeu	Nivel/Velocidad/Caudal	3	SF-04-03-EEBB_SB-Sant_Bartomeu	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
No	Caudalimetros	Alivios EBARs	SF-04-06-PR_SB-14	SF-04-06-PR_SB-14	Nivel/Velocidad/Caudal	3	SF-04-06-PR_SB-14	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
No	Caudalimetros	Alivios EBARs	SF-04-06-PR_SB-01	SF-04-06-PR_SB-01	Nivel/Velocidad/Caudal	3	SF-04-06-PR_SB-01	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
No	Caudalimetros	Alivios EBARs	SF-04-12-PR_SB-01	SF-04-12-PR_SB-01	Nivel/Velocidad/Caudal	3	SF-04-12-PR_SB-01	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
No	Caudalimetros	Alivios EBARs	SF-04-12-SB-EEBB-Aigues de Sabadell 5	SF-04-12-SB-EEBB-Aigues de Sabadell 5	Nivel/Velocidad/Caudal	3	SF-04-12-SB-EEBB-Aigues de Sabadell 5	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
No	Caudalimetros	Alivios EBARs	SF-03-19-EB-SB-01	SF-03-19-EB-SB-01	Nivel/Velocidad/Caudal	3	SF-03-19-EB-SB-01	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
No	Caudalimetros	Alivios EBARs	SF-03-12-PR_SB-02	SF-03-12-PR_SB-02	Nivel/Velocidad/Caudal	3	SF-03-12-PR_SB-02	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
No	Caudalimetros	Alivios EBARs	SF-EEBB_SB-Carrer_del_Pi	SF-EEBB_SB-Carrer_del_Pi	Nivel/Velocidad/Caudal	3	SF-EEBB_SB-Carrer_del_Pi	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
No	Caudalimetros	Alivios EBARs	SF-EEBB_SB-Placa_de_Avellaner	SF-EEBB_SB-Placa_de_Avellaner	Nivel/Velocidad/Caudal	3	SF-EEBB_SB-Placa_de_Avellaner	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
No	Caudalimetros	Alivios EBARs	SF-03-14-EEBB_SB_Rafamans-57	SF-03-14-EEBB_SB_Rafamans-57	Nivel/Velocidad/Caudal	3	SF-03-14-EEBB_SB_Rafamans-57	5 min	8 horas / 5 min	Decimal	SOFREL / Edge	EDAR Prat	72h	
Sí	Calidad alivios RED	RED COLECTORES	EBAR CORNELLÀ	EBAR CORNELLÀ	EQS alivios RED	4	EBAR CORNELLÀ	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	Calidad alivios RED	RED COLECTORES	EBAR INTERCEPTOR DE CASTELLDEFELS	EBAR INTERCEPTOR DE CASTELLDEFELS	EQS alivios RED	4	EBAR INTERCEPTOR DE CASTELLDEFELS	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Gavà	EDAR Gavá	72h	
Sí	Calidad alivios RED	RED COLECTORES	EBAR CAN RAFAMANS	EBAR CAN RAFAMANS	EQS alivios RED	4	EBAR CAN RAFAMANS	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Sant Feliu	EDAR Sant Feliu	72h	
Sí	Calidad alivios RED	RED COLECTORES	EBAR BAC DE RODA	EBAR BAC DE RODA	EQS alivios RED	4	EBAR BAC DE RODA	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Besos	EDAR Besos	72h	
Sí	Calidad alivios RED	RED COLECTORES	EBAR SANT ADRIÀ	EBAR SANT ADRIÀ	EQS alivios RED	4	EBAR SANT ADRIÀ	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Besos	EDAR Besos	72h	
Sí	Caudales vertidos EDAR	EDAR	EDAR Prat Vertido/Alivio (Lado Prat)	EDAR Prat Vertido/Alivio (Lado Prat)	Caudales vertidos EDAR	3	EDAR Prat Vertido/Alivio (Lado Prat)	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	Caudales vertidos EDAR	EDAR	EDAR Prat Vertido / Alivio (Lado Barcelona)	EDAR Prat Vertido / Alivio (Lado Barcelona)	Caudales vertidos EDAR	3	EDAR Prat Vertido / Alivio (Lado Barcelona)	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
No	Caudales vertidos EDAR	EDAR	EDAR Gavá	EDAR Gavá	Caudales vertidos EDAR	3	EDAR Gavá	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Gavà	EDAR Gavá	72h	
No	Caudales vertidos EDAR	EDAR	EDAR Sant Feliu	EDAR Sant Feliu	Caudales vertidos EDAR	3	EDAR Sant Feliu	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Sant Feliu	EDAR Sant Feliu	72h	
No	Caudales vertidos EDAR	EDAR	EDAR Besos	EDAR Besos	Caudales vertidos EDAR	3	EDAR Besos	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Besos	EDAR Besos	72h	
No	Caudales vertidos EDAR	EDAR	EDAR Vallvidrera	EDAR Vallvidrera	Caudales vertidos EDAR	3	EDAR Vallvidrera	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Sant Feliu	EDAR Sant Feliu	72h	
No	Caudales vertidos EDAR	EDAR	EDAR Montcada	EDAR Montcada	Caudales vertidos EDAR	3	EDAR Montcada	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Montcada	EDAR Montcada	72h	
No	Caudales vertidos EDAR	EDAR	EDAR Begues	EDAR Begues	Caudales vertidos EDAR	3	EDAR Begues	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Gavà	EDAR Gavá	72h	24
Sí	Calidad vertidos EDAR	EDAR	EDAR EL PRAT (Salida secundario lado Barcelona)		Calidad vertido	4	EDAR EL PRAT (Salida secundario lado Barcelona)	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	Calidad vertidos EDAR	EDAR	EDAR EL PRAT (Salida secundario lado Prat)		Calidad vertido	4	EDAR EL PRAT (Salida secundario lado Prat)	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	Calidad vertidos EDAR	EDAR	EDAR GAVÀ (Salida Zona IFAS)		Calidad vertido	2	EDAR GAVÀ (Salida Zona IFAS)	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Gavà	EDAR Gavá	72h	
Sí	Calidad vertidos EDAR	EDAR	EDAR GAVÀ (Salida Zona MBR)		Calidad vertido	2	EDAR GAVÀ (Salida Zona MBR)	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Gavà	EDAR Gavá	72h	
Sí	Calidad vertidos EDAR	EDAR	EDAR SANT FELIU (Salida secundario)		Calidad vertido	3	EDAR SANT FELIU (Salida secundario)	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Sant Feliu	EDAR Sant Feliu	72h	
No	Sonda turbidez HACH	EDAR	EDAR Prat	Turbidez salida decantación secundaria lado BCN	Turbidez	1	PLC ??	5 min	8 horas / 5 min	Decimal	PLC ??	EDAR Prat	72h	
No	Analizador Amonio HACH	EDAR	EDAR Prat	Amonio salida decantación secundaria lado BCN	Amonio	1	PLC ??	5 min	8 horas / 5 min	Decimal	PLC ??	EDAR Prat	72h	
No	Analizador Nitratos HACH	EDAR	EDAR Prat	Nitrato salida decantación secundaria lado BCN	Nitrato	1	PLC ??	5 min	8 horas / 5 min	Decimal	PLC ??	EDAR Prat	72h	
No	Sonda turbidez HACH	EDAR	EDAR Gavá	Salida IFAS	Turbidez	1	PLC ??	5 min	8 horas / 5 min	Decimal	PLC ??	EDAR Gavá	72h	
No	Sonda turbidez HACH	EDAR	EDAR Gavá	Salida MBR	Turbidez	1	PLC ??	5 min	8 horas / 5 min	Decimal	PLC ??	EDAR Gavá	72h	
No	Analizador Amonio HACH	EDAR	EDAR Gavá	Salida MBR	Amonio	1	PLC ??	5 min	8 horas / 5 min	Decimal	PLC ??	EDAR Gavá	72h	
No	Analizador Nitratos HACH	EDAR	EDAR Gavá	Salida MBR	Nitrato	1	PLC ??	5 min	8 horas / 5 min	Decimal	PLC ??	EDAR Gavá	72h	
No	Analizador Fosforo HACH	EDAR	EDAR Gavá	Salida MBR	Fósforo	1	PLC ??	5 min	8 horas / 5 min	Decimal	PLC ??	EDAR Gavá	72h	
No	Analizador Amonio HACH	EDAR	EDAR Sant Feliu	Salida decantación secundaria	Amonio	1	PLC ??	5 min	8 horas / 5 min	Decimal	PLC ??	EDAR Sant Feliu	72h	
No	Analizador Nitratos HACH	EDAR	EDAR Sant Feliu	Salida decantación secundaria	Nitrato	1	PLC ??	5 min	8 horas / 5 min	Decimal	PLC ??	EDAR Sant Feliu	72h	
No	Analizador Fosforo HACH	EDAR	EDAR Sant Feliu	Salida decantación secundaria	Fósforo	1	PLC ??	5 min	8 horas / 5 min	Decimal	PLC ??	EDAR Sant Feliu	72h	
No	Sonda MES	EDAR	EDAR Sant Feliu	Salida decantación secundaria	Materia en Suspensión	1	PLC ??	5 min	8 horas / 5 min	Decimal	PLC ??	EDAR Sant Feliu	72h	27
Sí	Caudales alivios EDAR	EDAR	EDAR GAVÀ (Emisario - Alivio Pluviales)		Caudal alivio	1	PLC Pooling EDAR Gavà	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Gavà	EDAR Gavá	72h	
Sí	Caudales alivios EDAR	EDAR	EDAR MONTCADA (Alivio entrada Biológico)		Caudal alivio	1	PLC Pooling EDAR Montcada	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Montcada	EDAR Montcada	72h	
Sí	Caudales alivios EDAR	EDAR	EDAR PRAT (Alivio Bombeo Intermedio)		Caudal alivio	1	PLC Pooling EDAR Prat	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	Caudales alivios EDAR	EDAR	EDAR PRAT (Alivio salida desarenadores - lado Barcelona)		Caudal alivio	1	PLC Pooling EDAR Prat	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
Sí	Caudales alivios EDAR	EDAR	EDAR PRAT (Alivio salida desarenadores - lado Prat)		Caudal alivio	1	PLC Pooling EDAR Prat	5 min	8 horas / 5 min	Decimal	PLC Pooling EDAR Prat	EDAR Prat	72h	
No	PLC	EDAR	EDAR Vallvidrera	Caudal alivio	Caudal	1	PLC ??	5 min	8 horas / 5 min	Decimal	PLC ??	EDAR Vallvidrera	72h	
No	PLC	EDAR	EDAR Begues	Caudal alivio	Caudal	1	PLC ??	5 min	8 horas / 5 min	Decimal	PLC ??	EDAR Begues	72h	7
						11.285								

			Adquisición de datos PLC frecuencia 10 segundos		Envío de datos MQTT frecuencia 1 minuto	
Ubicación del Edge	Frecuencia envio desde Edge	SUM de Numero variables	Tasa de datos (Bps)	Ancho de banda (kbps)	Tasa de datos (Bps)	Ancho de banda (kbps)
		11.285	4514,000	43,334	4702,083	45,140
EDAR Begues	5 min	1	0,400	0,004	0,417	0,004
EDAR Besos	5 min	221	88,400	0,849	92,083	0,884
EDAR Gavá	15 minutos	2800	1120,000	10,752	1166,667	11,200
	5 min	328	131,200	1,260	136,667	1,312
EDAR Montcada	5 min	4	1,600	0,015	1,667	0,016
EDAR Prat	15 minutos	4680	1872,000	17,971	1950,000	18,720
	5 min	717	286,800	2,753	298,750	2,868
EDAR Sant Feliu	15 minutos	2080	832,000	7,987	866,667	8,320
	5 min	449	179,600	1,724	187,083	1,796
EDAR Vallvidrera	5 min	5	2,000	0,019	2,083	0,020
		9042	3616,8	34,72128	3767,5	36,168

Anexo 5: Planificación (.pdf)

PLANIFICACIÓN IMPLANTACIÓN PLATAFORMA IIoT

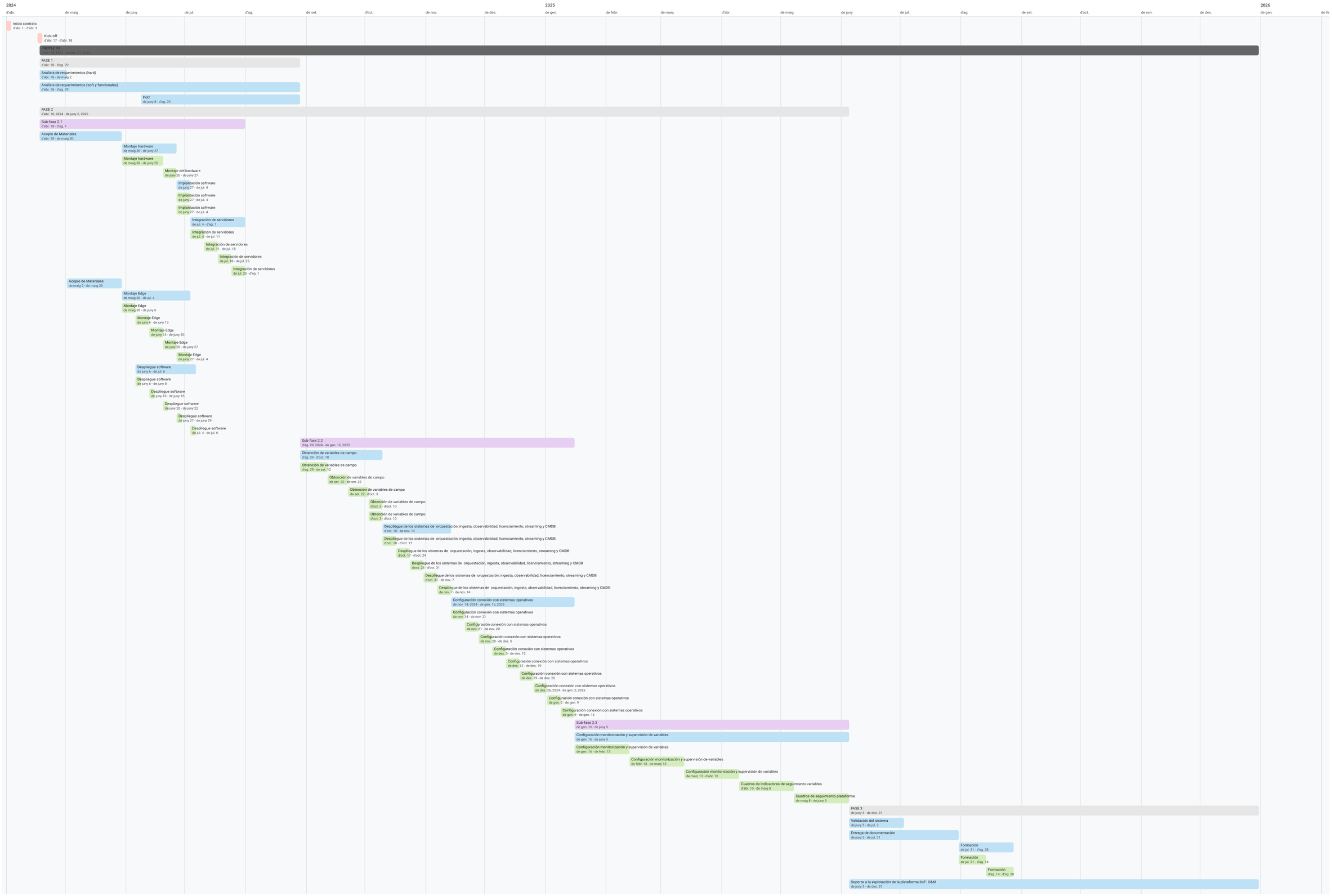
Tarea	Sub-Tarea	Fecha inicio	Fecha fin	Duración (día)	Duración (semana)
Inicio contrato		1/04/2024	2/04/2024	1,0	0,1
Kick-off		17/04/2024	18/04/2024	1,0	0,1
PROYECTO		18/04/2024	31/12/2025	622	88,9
FASE 1	ANÁLISIS Y DISEÑO	18/04/2024	29/08/2024	133	19,0
Análisis de requerimientos (hard)		18/04/2024	2/05/2024	14,0	2,0
Análisis de requerimientos (soft y funcionales)		18/04/2024	29/08/2024	133,0	19,0
PoC		8/06/2024	29/08/2024	81,2	11,6
FASE 2		18/04/2024	5/06/2025	413,0	59,0
Sub-fase 2.1	IMPLANTACIÓN HARDWARE Y SOFTWARE	18/04/2024	1/08/2024	105,0	15,0
Acopio de Materiales	TI-Ciber	18/04/2024	30/05/2024	42,0	6,0
Montaje hardware	TI-Ciber	30/05/2024	27/06/2024	28,0	4,0
Montaje hardware	TI	30/05/2024	20/06/2024	21,0	3,0
Montaje del hardware	Ciber	20/06/2024	27/06/2024	7,0	1,0
Implantación software	TI-Ciber	27/06/2024	4/07/2024	7,0	1,0
Implantación software	TI	27/06/2024	4/07/2024	7,0	1,0
Implantación software	Ciber	27/06/2024	4/07/2024	7,0	1,0
Integración de servidores	TI	4/07/2024	1/08/2024	28,0	4,0
Integración de servidores	CPD	4/07/2024	11/07/2024	7,0	1,0
Integración de servidores	EDAR Gavá	11/07/2024	18/07/2024	7,0	1,0
Integración de servidores	EDAR Sant Feliú	18/07/2024	25/07/2024	7,0	1,0
Integración de servidores	EDAR Montcada	25/07/2024	1/08/2024	7,0	1,0
Acopio de Materiales	OT	2/05/2024	30/05/2024	28,0	4,0
Montaje Edge	OT	30/05/2024	4/07/2024	35,0	5,0
Montaje Edge	EDAR Baix Llobregat	30/05/2024	6/06/2024	7,0	1,0
Montaje Edge	EDAR Sant Feliú	6/06/2024	13/06/2024	7,0	1,0
Montaje Edge	EDAR Gavá	13/06/2024	20/06/2024	7,0	1,0
Montaje Edge	EDAR Besós	20/06/2024	27/06/2024	7,0	1,0
Montaje Edge	EDAR Montcada	27/06/2024	4/07/2024	7,0	1,0
Despliegue software	OT	6/06/2024	6/07/2024	30,8	4,4
Despliegue software	EDAR Baix Llobregat	6/06/2024	8/06/2024	2,8	0,4
Despliegue software	EDAR Sant Feliú	13/06/2024	15/06/2024	2,8	0,4
Despliegue software	EDAR Gavá	20/06/2024	22/06/2024	2,8	0,4
Despliegue software	EDAR Besós	27/06/2024	29/06/2024	2,8	0,4

PLANIFICACIÓN IMPLANTACIÓN PLATAFORMA IIoT

Tarea	Sub-Tarea	Fecha inicio	Fecha fin	Duración (día)	Duración (semana)
Despliegue software	EDAR Montcada	4/07/2024	6/07/2024	2,8	0,4
Sub-fase 2.2	CONFIGURACIÓN DE LA PLATAFORMA IIoT	29/08/2024	16/01/2025	140,0	20,0
Obtención de variables de campo	OT	29/08/2024	10/10/2024	42,0	6,0
Obtención de variables de campo	Sistema Baix Llobregat	29/08/2024	12/09/2024	14,0	2,0
Obtención de variables de campo	Sistema Sant Feliú	12/09/2024	22/09/2024	10,5	1,5
Obtención de variables de campo	Sistema Gavá	22/09/2024	3/10/2024	10,5	1,5
Obtención de variables de campo	Sistema Besós	3/10/2024	10/10/2024	7,0	1,0
Obtención de variables de campo	Sistema Montcada	3/10/2024	10/10/2024	7,0	1,0
Despliegue de los sistemas de orquestación, ingesta, observabilidad, licenciamiento, streaming y CMDB	OT	10/10/2024	14/11/2024	35,0	5,0
Despliegue de los sistemas de orquestación, ingesta, observabilidad, licenciamiento, streaming y CMDB	Ingesta	10/10/2024	17/10/2024	7,0	1,0
Despliegue de los sistemas de orquestación, ingesta, observabilidad, licenciamiento, streaming y CMDB	Orquestación	17/10/2024	24/10/2024	7,0	1,0
Despliegue de los sistemas de orquestación, ingesta, observabilidad, licenciamiento, streaming y CMDB	Observabilidad	24/10/2024	31/10/2024	7,0	1,0
Despliegue de los sistemas de orquestación, ingesta, observabilidad, licenciamiento, streaming y CMDB	Streaming	31/10/2024	7/11/2024	7,0	1,0
Despliegue de los sistemas de orquestación, ingesta, observabilidad, licenciamiento, streaming y CMDB	CMDB	7/11/2024	14/11/2024	7,0	1,0
Configuración conexión con sistemas operativos		14/11/2024	16/01/2025	63,0	9,0

PLANIFICACIÓN IMPLANTACIÓN PLATAFORMA IIoT					
Tarea	Sub-Tarea	Fecha inicio	Fecha fin	Duración (día)	Duración (semana)
Configuración conexión con sistemas operativos	SCADA	14/11/2024	21/11/2024	7,0	1,0
Configuración conexión con sistemas operativos	Gemelo digital	21/11/2024	28/11/2024	7,0	1,0
Configuración conexión con sistemas operativos	Datos meteorológicos	28/11/2024	5/12/2024	7,0	1,0
Configuración conexión con sistemas operativos	SITEC	5/12/2024	12/12/2024	7,0	1,0
Configuración conexión con sistemas operativos	LIMS	12/12/2024	19/12/2024	7,0	1,0
Configuración conexión con sistemas operativos	Plataformas energía	19/12/2024	26/12/2024	7,0	1,0
Configuración conexión con sistemas operativos	Plataforma monitorización avanzada consumos eléctricos	26/12/2024	2/01/2025	7,0	1,0
Configuración conexión con sistemas operativos	Configuración DCDC	2/01/2025	9/01/2025	7,0	1,0
Configuración conexión con sistemas operativos	Configuración Otros (AQMOS, IFM, Artificial Vision...)	9/01/2025	16/01/2025	7,0	1,0
Sub-fase 2.3	CONFIGURACIÓN MONITORIZACIÓN, SUPERVISIÓN Y CUADROS DE MANDO	16/01/2025	5/06/2025	140,0	20,0
Configuración monitorización y supervisión de variables		16/01/2025	5/06/2025	140,0	20,0
Configuración monitorización y supervisión de variables	Definición de pantallas	16/01/2025	13/02/2025	28,0	4,0
Configuración monitorización y supervisión de variables	Monitorización de variables	13/02/2025	13/03/2025	28,0	4,0
Configuración monitorización y supervisión de variables	Campo de definición: eventos, alarmas	13/03/2025	10/04/2025	28,0	4,0
Cuadros de indicadores de seguimiento variables	Cuadros de mando	10/04/2025	8/05/2025	28,0	4,0
Cuadros de seguimiento plataforma		8/05/2025	5/06/2025	28,0	4,0
FASE 3	CIERRE PROYECTO Y SOPORTE A LA OPERACIÓN	5/06/2025	31/12/2025	209,0	29,9

PLANIFICACIÓN IMPLANTACIÓN PLATAFORMA IIoT					
Tarea	Sub-Tarea	Fecha inicio	Fecha fin	Duración (día)	Duración (semana)
Validación del sistema		5/06/2025	3/07/2025	28,0	4,0
Entrega de documentación		5/06/2025	31/07/2025	56,0	8,0
Formación		31/07/2025	28/08/2025	28,0	4,0
Formación	Mantenimiento plataforma IIoT	31/07/2025	14/08/2025	14,0	2,0
Formación	Operación plataforma IIoT	14/08/2025	28/08/2025	14,0	2,0
Soporte a la explotación de la plataforma IIoT: O&M		5/06/2025	31/12/2025	209,0	29,9


2024
d'abr.
de maig
de juny
de jul.
d'ag.
de set.
d'oct.
de nov.
de des.
2025
de gen.
de febr.
de març
d'abr.
de maig
de juny
de jul.
d'ag.
de set.
d'oct.
de nov.
de des.
2026
de gen.
de fe
Inicio contrato
d'abr. 1 - d'abr. 2
Kick-off
d'abr. 17 - d'abr. 18
PROYECTO
d'abr. 18, 2024 - de des. 30, 2026
FASE 1
d'abr. 18 - d'ag. 29
Análisis de requerimientos (hard)
d'abr. 18 - de maig 2
Análisis de requerimientos (soft y funcionales)
d'abr. 18 - d'ag. 29
PoC
de juny 8 - d'ag. 29
FASE 2
d'abr. 18, 2024 - de juny 5, 2025
Sub-fase 2.1
d'abr. 18 - d'ag. 1
Acopio de Materiales
d'abr. 18 - de maig 30
Montaje hardware
de maig 30 - de juny 27
Montaje hardware
de maig 30 - de juny 20
Montaje del hardware
de juny 20 - de juny 27
Implantación software
de juny 27 - de jul. 4
Implantación software
de juny 27 - de jul. 4
Implantación software
de juny 27 - de jul. 4
Integración de servidores
de jul. 4 - d'ag. 1
Integración de servidores
de jul. 4 - de jul. 11
Integración de servidores
de jul. 11 - de jul. 18
Integración de servidores
de jul. 18 - de jul. 25
Integración de servidores
de jul. 25 - d'ag. 1
Acopio de Materiales
de maig 2 - de maig 30
Montaje Edge
de maig 30 - de jul. 4
Montaje Edge
de maig 30 - de juny 6
Montaje Edge
de juny 6 - de juny 13
Montaje Edge
de juny 13 - de juny 20
Montaje Edge
de juny 20 - de juny 27
Montaje Edge
de juny 27 - de jul. 4
Despliegue software
de juny 6 - de jul. 6
Despliegue software
de juny 6 - de juny 8
Despliegue software
de juny 13 - de juny 15
Despliegue software
de juny 20 - de juny 22
Despliegue software
de juny 27 - de juny 29
Despliegue software
de jul. 4 - de jul. 6
Sub-fase 2.2
d'ag. 29, 2024 - de gen. 16, 2025
Obtención de variables de campo
d'ag. 29 - d'oct. 10
Obtención de variables de campo
d'ag. 29 - de set. 12
Obtención de variables de campo
de set. 12 - de set. 22
Obtención de variables de campo
de set. 22 - d'oct. 3
Obtención de variables de campo
d'oct. 3 - d'oct. 10
Obtención de variables de campo
d'oct. 3 - d'oct. 10
Despliegue de los sistemas de orquestación, ingesta, observabilidad, licenciamiento, streaming y CMDB
d'oct. 10 - de nov. 14
Despliegue de los sistemas de orquestación, ingesta, observabilidad, licenciamiento, streaming y CMDB
d'oct. 10 - d'oct. 17
Despliegue de los sistemas de orquestación, ingesta, observabilidad, licenciamiento, streaming y CMDB
d'oct. 17 - d'oct. 24
Despliegue de los sistemas de orquestación, ingesta, observabilidad, licenciamiento, streaming y CMDB
d'oct. 24 - d'oct. 31
Despliegue de los sistemas de orquestación, ingesta, observabilidad, licenciamiento, streaming y CMDB
d'oct. 31 - de nov. 7
Despliegue de los sistemas de orquestación, ingesta, observabilidad, licenciamiento, streaming y CMDB
de nov. 7 - de nov. 14
Configuración conexión con sistemas operativos
de nov. 14, 2024 - de gen. 16, 2025
Configuración conexión con sistemas operativos
de nov. 14 - de nov. 21
Configuración conexión con sistemas operativos
de nov. 21 - de nov. 28
Configuración conexión con sistemas operativos
de nov. 28 - de des. 5
Configuración conexión con sistemas operativos
de des. 5 - de des. 12
Configuración conexión con sistemas operativos
de des. 12 - de des. 19
Configuración conexión con sistemas operativos
de des. 19 - de des. 26
Configuración conexión con sistemas operativos
de des. 26, 2024 - de gen. 2, 2025
Configuración conexión con sistemas operativos
de gen. 2 - de gen. 9
Configuración conexión con sistemas operativos
de gen. 9 - de gen. 16
Sub-fase 2.3
de gen. 16 - de juny 5
Configuración monitorización y supervisión de variables
de gen. 16 - de juny 5
Configuración monitorización y supervisión de variables
de gen. 16 - de febr. 13
Configuración monitorización y supervisión de variables
de febr. 13 - de març 13
Configuración monitorización y supervisión de variables
de març 13 - d'abr. 10
Cuadros de indicadores de seguimiento variables
d'abr. 10 - de maig 8
Cuadros de seguimiento plataforma
de maig 8 - de juny 5
FASE 3
de juny 5 - de des. 31
Validación del sistema
de juny 5 - de jul. 3
Entrega de documentación
de juny 5 - de jul. 31
Formación
de jul. 31 - d'ag. 28
Formación
de jul. 31 - d'ag. 14
Formación
d'ag. 14 - d'ag. 28
Soporte a la explotación de la plataforma IIoT: O&M
de juny 5 - de des. 31

Anexo 6: Presupuesto (.pdf)

Ítem	Descripción	Uds	Precio Ud ofertado	Precio ofertado
	Lote 1 - IIoT - OT			
	Nodos Edge			
1	Suministro HW - Edge - Celeron 4C/4T - 16GB RAM - 512GB SSD	6		0,00 €
2	Suministro SW - Licencias - IIoT Data Adquisition System (anual)	5		0,00 €
3	Instalación y PeM - Edge - Incluye material eléctrico para la adaptación al armario industrial	5		0,00 €
4	Instalación y PeM - Edge - Enroll de nodo Edge en IIoT Digitalization Platform y Orquestador Industrial	5		0,00 €
	Subtotal Nodos Edge			**0,00 €**
	Data Streaming			
5	Instalación y PeM - Edge - Instalación y configuración de nodos de Data Streaming	1		0,00 €
	Subtotal Data Sreaming			**0,00 €**
	Orquestación			
6	Suministro SW - Licencias Orquestador - Orquestador Industrial (Soporte 8x5 - <12 horas) (anual)	2		0,00 €
7	Suministro SW - Licencias Orquestador - Orquestador Industrial - New Node (anual - 5 ud)	2		0,00 €
8	Instalación y PeM - Edge - Instalación y configuración de nodos de Orquestación	1		0,00 €
	Subtotal Orquestación			**0,00 €**
	IIoT Platform			
9	Suministro SW - Licencias - IIoT Digitalization Platform - Subscription (anual)	2		0,00 €
10	Instalación y PeM - Edge - Configuración y puesta en servico - IIoT Digitalization Platform	1		0,00 €
	Subtotal IIoT Platform			**0,00 €**
	Desarrollo componentes de la plataforma IIoT			
11	Diseño - Ingeniería de detalle de los componentes de la plataforma IIoT	1		0,00 €
12	Desarrollo - Configuración de activos en plataforma	1		0,00 €
13	Desarrollo - Configuración de sistemas de ingesta en plataforma	1		0,00 €
14	Desarrollo - Configuración de caminos en data streaming	1		0,00 €
15	Desarrollo - Diseño y configuración de dashboarding	1		0,00 €
16	Desarrollo - Integración de sistemas (desarrollos/setting para la integración de sistemas externos/internos)	1		0,00 €
	Subtotal Desarrollo componentes de la plataforma IIoT			**0,00 €**
	Costes generales de proyecto			
17	Desarrollo - Dirección de proyecto	1		0,00 €
19	Documentación de mantenimiento y configuración	1		0,00 €
20	Formación	1		0,00 €
18	Partida en alzada a justificar - imprevistos suministros, programaciones y adaptaciones	1	65.343,00€	65.343,00 €
	Subtotal Costes generales de proyecto			**65.343,00 €**
	TOTAL Lote 1 - IIoT - OT			**65.343,00 €**
	Lote 2 - IIoT - TI / Ciberseguridad			
	Infraestructura TI			
21	Infraestructura Plataforma de virtualización	1		0,00 €
26	Partida en alzada a justificar - suministro infraestructura TI	1	20.224,40€	20.224,40 €
	Subtotal Infraestructura TI			**20.224,40 €**
	Ciberseguridad			
22	Suministro licencias McAfee Application Control (ACD) (Perpetual) - 3 años/ud	30		0,00 €
23	Suministro licencias McAfee Application Control (ACD) (Perpetual) - 3 años/ud	30		0,00 €
24	Suministro licencias FireEye Endpoint Security - 3 años/ud	30		0,00 €
25	Suministro licencias Deep Security - Malware Prevention y Network Security - per Server (VM) - 3 años/ud	5		0,00 €
26	Partida en alzada a justificar - suministro otras licencias ciberseguridad	1	2.400,00€	2.400,00 €
	Subtotal Ciberseguridad			**2.400,00 €**
	TOTAL Lote 2 - TI / Ciberseguridad			**22.624,40 €**
	Lote 3 - PMO SCI			
	PMO SCI			
26	PMO SCI horas	1.572		0,00 €
	Subtotal PMO SCI			
	TOTAL Lote 3 - PMO SCI			**151.020,00 €**
	PRESUPUESTO MÁXIMO			**1.118.661,40 €**
	PRESUPUESTO MÁXIMO LICENCIAMIENTO ANUAL			**120.700,00 €**

Anexo 7: Modelo de acta (.pdf)

FECHA Y HORA:	*dd/mm/aaaa (00:00 h a 00:00 h)*	**OBJETO de la reunión:**	
LUGAR:		**TIPO DE REUNIÓN:**	☐ Inicial ☐ Cierre ☐ Seguimiento ☐ Extraordinaria ☐ Otra:……
ORGANIZADOR/A:		**ELABORADOR/A ACTA:**	

ASISTENTES:	**EXCUSADOS/AS**

ORDEN DEL DÍA:

1. **REVISIÓN Y APROBACIÓN ACTA ANTERIOR**
2. **SEGUIMIENTO DEL PROYECTO**
3. **INCIDENCIAS**
4. **INDICADORES DE SERVICIO Y ACCIONES CORRECTORAS**
5. **OTROS**
6. **CONCLUSIONES Y ACUERDOS**

Las conclusiones y acuerdos de la reunión se recogen en la siguiente tabla:

CONCLUSIONES Y ACUERDOS	**RESPONSABLE**	**FECHA**	**ESTADO** (En plazo - Realizada - Pendiente)